ISC.SSCP.v2022-01-29.q657

Exam Code:	SSCP
Exam Name:	System Security Certified Practitioner (SSCP)
Certification Provider:	ISC
Free Question Number:	657
Version:	v2022-01-29
# of views:	17539
# of Questions views:	6570
https://www.exam-tests.com/SSCP-exam/ISC.SSCP.v2022-01-29.q657.html	

NEW QUESTION: 1
In an organization where there are frequent personnel changes, non-discretionary access control using Role Based Access Control (RBAC) is useful because:
A. people need not use discretion
B. the access controls are based on the individual's role or title within the organization.
C. the access controls are not based on the individual's role or title within the organization
D. the access controls are often based on the individual's role or title within the organization
Answer: B (LEAVE A REPLY)
Explanation/Reference:
In an organization where there are frequent personnel changes, non-discretionary access control (also called Role Based Access Control) is useful because the access controls are based on the individual's role or title within the organization. You can easily configure a new employee acces by assigning the user to a role that has been predefine. The user will implicitly inherit the permissions of the role by being a member of that role.
These access permissions defined within the role do not need to be changed whenever a new person takes over the role.
Another type of non-discretionary access control model is the Rule Based Access Control (RBAC or RuBAC) where a global set of rule is uniformly applied to all subjects accessing the resources. A good example of RuBAC would be a firewall.
This question is a sneaky one, one of the choice has only one added word to it which is often. Reading questions and their choices very carefully is a must for the real exam. Reading it twice if needed is recommended.
Shon Harris in her book list the following ways of managing RBAC:
Role-based access control can be managed in the following ways:
Non-RBAC Users are mapped directly to applications and no roles are used. (No roles being used)
Limited RBAC Users are mapped to multiple roles and mapped directly to other types of applications that do not have role-based access functionality. (A mix of roles for applications that supports roles and

explicit access control would be used for applications that do not support roles) Hybrid RBAC Users are mapped to multiapplication roles with only selected rights assigned to those roles.
Full RBAC Users are mapped to enterprise roles. (Roles are used for all access being granted) NIST defines RBAC as:
Security administration can be costly and prone to error because administrators usually specify access control lists for each user on the system individually. With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles. Complexities introduced by mutually exclusive roles or role hierarchies are handled by the RBAC software, making security administration easier.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition McGraw-Hill.
and
http://csrc.nist.gov/groups/SNS/rbac/

NEW QUESTION: 2
Which of the following proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?
A. Direct evidence.
B. Circumstantial evidence.
C. Conclusive evidence.
D. Corroborative evidence.
Answer: (SHOW ANSWER)
Direct evidence can prove a fact all by itself and does not need backup information to refer to. When using direct evidence, presumptions are not required. One example of direct evidence is the testimony of a witness who saw a crime take place. Although this oral evidence would be secondary in nature, meaning a case could not rest on just it alone, it is also direct evidence, meaning the lawyer does not necessarily need to provide other evidence to back it up. Direct evidence often is based on information gathered from a witness's five senses.
The following answers are incorrect:
Circumstantial evidence. Is incorrect because Circumstantial evidence can prove an intermediate fact that can then be used to deduce or assume the existence of another fact. Conclusive evidence. Is incorrect because Conclusive evidence is irrefutable and cannot be contradicted. Conclusive evidence is very strong all by itself and does not require corroboration.
Corroborative evidence. Is incorrect because Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand on its own, but is used as a supplementary tool to help prove a primary piece of evidence.

NEW QUESTION: 3
What layer of the OSI/ISO model does Point-to-point tunnelling protocol (PPTP) work at?
A. Data link layer
B. Transport layer
C. Session layer
D. Network layer
Answer: (SHOW ANSWER)
PPTP operates at the data link layer (layer 2) of the OSI model and uses native PPP authentication and encryption services. Designed for individual client to server connections, it enables only a single point-to-point connection per session.
PPTP - Point-to-Point Tunneling Protocol - extends the Point to Point Protocol (PPP) standard for traditional dial-up networking. PPTP is best suited for the remote access applications of VPNs, but it also supports LAN internetworking.
PPTP operates at Layer 2 of the OSI model.
Using PPTP
PPTP packages data within PPP packets, then encapsulates the PPP packets within IP packets (datagrams) for transmission through an Internet-based VPN tunnel. PPTP supports data encryption and compression of these packets. PPTP also uses a form of General Routing Encapsulation (GRE) to get data to and from its final destination.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 95). and http://compnetworking.about.com/od/vpn/l/aa030103a.htm and http://technet.microsoft.com/en-us/library/cc768084.aspx

NEW QUESTION: 4
An alternative to using passwords for authentication in logical or technical access control is:
A. manage without passwords
B. biometrics
C. not there
D. use of them for physical access control
Answer: B (LEAVE A REPLY)
An alternative to using passwords for authentication in logical or technical access control is biometrics. Biometrics are based on the Type 3 authentication mechanism-something you are. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION: 5
The security of a computer application is most effective and economical in which of the following cases?
A. The system is optimized prior to the addition of security.

B. The system is procured off-the-shelf.
C. The system is customized to meet the specific security threat.
D. The system is originally designed to provide the necessary security.
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The earlier in the process that security is planned for and implement the cheaper it is. It is also much more efficient if security is addressed in each phase of the development cycle rather than an add-on because it gets more complicated to add at the end. If security plan is developed at the beginning it ensures that security won't be overlooked.
The following answers are incorrect:
The system is optimized prior to the addition of security. Is incorrect because if you wait to implement security after a system is completed the cost of adding security increases dramtically and can become much more complex.
The system is procured off-the-shelf. Is incorrect because it is often difficult to add security to off-the shelf systems.
The system is customized to meet the specific security threat. Is incorrect because this is a distractor. This implies only a single threat.

NEW QUESTION: 6
How can an individual/person best be identified or authenticated to prevent local masquarading attacks?
A. UserId and password
B. Smart card and PIN code
C. Two-factor authentication
D. Biometrics
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The only way to be truly positive in authenticating identity for access is to base the authentication on the physical attributes of the persons themselves (i.e., biometric identification). Physical attributes cannot be shared, borrowed, or duplicated. They ensure that you do identify the person, however they are not perfect and they would have to be supplemented by another factor.
Some people are getting thrown off by the term Masquarade. In general, a masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. Spoofing is another term used to describe this type of attack as well.
A UserId only provides for identification.
A password is a weak authentication mechanism since passwords can be disclosed, shared, written down, and more.

A smart card can be stolen and its corresponding PIN code can be guessed by an intruder. A smartcard can be borrowed by a friend of yours and you would have no clue as to who is really logging in using that smart card.

Any form of two-factor authentication not involving biometrics cannot be as reliable as a biometric system to identify the person.

Biometric identifying verification systems control people. If the person with the correct hand, eye, face, signature, or voice is not present, the identification and verification cannot take place and the desired action (i.e., portal passage, data, or resource access) does not occur.

As has been demonstrated many times, adversaries and criminals obtain and successfully use access cards, even those that require the addition of a PIN. This is because these systems control only pieces of plastic (and sometimes information), rather than people. Real asset and resource protection can only be accomplished by people, not cards and information, because unauthorized persons can (and do) obtain the cards and information.

Further, life-cycle costs are significantly reduced because no card or PIN administration system or personnel are required. The authorized person does not lose physical characteristics (i.e., hands, face, eyes, signature, or voice), but cards and PINs are continuously lost, stolen, or forgotten. This is why card access systems require systems and people to administer, control, record, and issue (new) cards and PINs. Moreover, the cards are an expensive and recurring cost.

NOTE FROM CLEMENT:

This question has been generating lots of interest. The keyword in the question is: Individual (the person) and also the authenticated portion as well.

I totally agree with you that Two Factors or Strong Authentication would be the strongest means of authentication. However the question is not asking what is the strongest mean of authentication, it is asking what is the best way to identify the user (individual) behind the technology. When answering questions do not make assumptions to facts not presented in the question or answers.

Nothing can beat Biometrics in such case. You cannot lend your fingerprint and pin to someone else, you cannot borrow one of my eye balls to defeat the Iris or Retina scan. This is why it is the best method to authenticate the user.

I think the reference is playing with semantics and that makes it a bit confusing. I have improved the question to make it a lot clearer and I have also improve the explanations attached with the question.

The reference mentioned above refers to authenticating the identity for access. So the distinction is being made that there is identity and there is authentication. In the case of physical security the enrollment process is where the identity of the user would be validated and then the biometrics features provided by the user would authenticate the user on a one to one matching basis (for authentication) with the reference contained in the database of biometrics templates. In the case of system access, the user might have to provide a username, a pin, a passphrase, a smart card, and then provide his biometric attributes.

Biometric can also be used for Identification purpose where you do a one to many match. You take a facial scan of someone within an airport and you attempt to match it with a large database of known criminal and terrorists. This is how you could use biometric for Identification.

There are always THREE means of authentication, they are:

Something you know (Type 1)
Something you have (Type 2)
Something you are (Type 3)
Reference(s) used for this question:
TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1) ,
2000, CRC Press, Chapter 1, Biometric Identification (page 7).
and
Search Security at http://searchsecurity.techtarget.com/definition/masquerade

NEW QUESTION: 7
What can be described as an imaginary line that separates the trusted components of the TCB from those elements that are NOT trusted?
A. The security kernel
B. The reference monitor
C. The security perimeter
D. The reference perimeter
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The security perimeter is the imaginary line that separates the trusted components of the kernel and the Trusted Computing Base (TCB) from those elements that are not trusted. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. The security kernel can be software, firmware or hardware components in a trusted system and is the actual instantiation of the reference monitor. The reference perimeter is not defined and is a distracter.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION: 8
In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?
A. Known-plaintext attack
B. Ciphertext-only attack
C. Chosen-Ciphertext attack
D. Plaintext-only attack
Answer: (SHOW ANSWER)
In a ciphertext-only attack, the attacker has the ciphertext of several messages encrypted with the same encryption algorithm. Its goal is to discover the plaintext of the messages by figuring out the key used in the encryption process. In a known-plaintext attack, the attacker has the plaintext and the ciphertext of one or more messages. In a chosen-ciphertext attack, the attacker can chose the ciphertext to be decrypted and has access to the resulting plaintext.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 578).

NEW QUESTION: 9
In the context of network enumeration by an outside attacker and possible Distributed Denial of Service (DDoS) attacks, which of the following firewall rules is not appropriate to protect an organization's internal network?
A. Allow echo reply outbound
B. Allow echo request outbound
C. Drop echo request inbound
D. Allow echo reply inbound
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Echo replies outbound should be dropped, not allowed. There is no reason for any internet users to send ICMP ECHO Request to your interal hosts from the internet. If they wish to find out if a service is available, they can use a browser to connect to your web server or simply send an email if they wish to test your mail service.
Echo replies outbound could be used as part of the SMURF amplification attack where someone will send ICMP echo requests to gateways broadcast addresses in order to amplify the request by X number of users sitting behind the gateway.
By allowing inbound echo requests and outbound echo replies, it makes it easier for attackers to learn about the internal network as well by performing a simply ping sweep. ICMP can also be used to find out which host has been up and running the longest which would indicates which patches are missing on the host if a critical patch required a reboot.
ICMP can also be use for DDoS attacks, so you should strictly limit what type of ICMP traffic would be allowed to flow through your firewall.
On top of all this, tools such as LOKI could be use as a client-server application to transfer files back and forward between the internat and some of your internal hosts. LOKI is a client/server program published in the online publication Phrack . This program is a working proof-of-concept to demonstrate that data can be transmitted somewhat secretly across a network by hiding it in traffic that normally does not contain payloads. The example code can tunnel the equivalent of a Unix RCMD/RSH session in either ICMP echo request (ping) packets or UDP traffic to the DNS port. This is used as a back door into a Unix system after root access has been compromised. Presence of LOKI on a system is evidence that the system has been compromised in the past.
The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.
The following answers are incorrect:
Allow echo request outbound The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.
Drop echo request inbound There is no need for anyone on the internet to attempt pinging your internal hosts.

Allow echo reply inbound The outbound echo request and inbound echo reply allow internal users to verify connectivity with external hosts.
Reference(s) used for this question:
http://www.phrack.org/issues.html?issue=49&id=6
STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 10: The Perfect Firewall.

NEW QUESTION: 10
Which of the following is NOT a true statement regarding the implementaton of the 3DES modes?
A. DES-EEE1 uses one key
B. DES-EEE2 uses two keys
C. DES-EEE3 uses three keys
D. DES-EDE2 uses two keys
Answer: A (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
There is no DES mode call DES-EEE1. It does not exist.
The following are the correct modes for triple-DES (3DES):
DES-EEE3 uses three keys for encryption and the data is encrypted, encrypted, encrypted; DES-EDE3 uses three keys and encrypts, decrypts and encrypts data.
DES-EEE2 and DES-EDE2 are the same as the previous modes, but the first and third operations use the same key.
Reference(s) used for this question:
Shon Harris, CISSP All In One (AIO) book, 6th edition , page 808
and
Official ISC2 Guide to the CISSP CBK, 2nd Edition (2010) , page 344-345

NEW QUESTION: 11
What is the main goal of a risk management program?
A. To help managers find the correct cost balance between risks and countermeasures
B. None of the above
C. To evaluate appropriate risk mitigation scenarios
D. To develop a disaster recovery plan
E. To calculate ALE formulas
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which of the following type of cryptography is used when both parties use the same key to communicate securely with each other?
A. Symmetric Key Cryptography
B. PKI - Public Key Infrastructure

C. Diffie-Hellman
D. DSS - Digital Signature Standard
Answer: A (LEAVE A REPLY)
Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext (sender) and decryption of ciphertext (receiver). The keys may be identical, in practice, they represent a shared secret between two or more parties that can be used to maintain a private information link.
This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. This is also known as secret key encryption. In symmetric key cryptography, each end of the conversation must have the same key or they cannot decrypt the message sent to them by the other party.
Symmetric key crypto is very fast but more difficult to manage due to the need to distribute the key in a secure means to all parts needing to decrypt the data. There is no key management built within Symmetric crypto.
PKI provides CIA - Confidentiality (Through encryption) Integrity (By guaranteeing that the message hasn't change in transit) and Authentication (Non-repudiation). Symmetric key crypto provides mostly Confidentiality.
The following answers are incorrect:
-PKI - Public Key Infrastructure: This is the opposite of symmetric key crypto. Each side in PKI has their own private key and public key. What one key encrypt the other one can decrypt. You make use of the receiver public key to communicate securely with a remote user. The receiver will use their matching private key to decrypt the data.
-Diffie-Hellman: Sorry, this is an asymmetric key technique. It is used for key agreement over an insecure network such as the Internet. It allows two parties who has never met to negotiate a secret key over an insecure network while preventing Man-In-The-Middle (MITM) attacks.
-DSS - Digital Signature Standard: Sorry, this is an asymmetric key technique.
The following reference(s) was used to create this question: To learn more about this questions and 100% of the Security+ CBK, subscribe to our Holistic Computer Based Tutorial (CBT) on our Learning Management System at: http://www.cccure.tv and http://en.wikipedia.org/wiki/Symmetric-key_algorithm

NEW QUESTION: 13
Which of the following service is a distributed database that translate host name to IP address to IP address to host name?
A. DNS
B. FTP
C. SSH
D. SMTP
Answer: (SHOW ANSWER)
The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the

numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

For your exam you should know below information general Internet terminology:

Network access point - Internet service providers access internet using net access point.A Network Access Point (NAP) was a public network exchange facility where Internet service providers (ISPs) connected with one another in peering arrangements. The NAPs were a key component in the transition from the 1990s NSFNET era (when many networks were government sponsored and commercial traffic was prohibited) to the commercial Internet providers of today. They were often points of considerable Internet congestion.

Internet Service Provider (ISP) - An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, nonprofit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, co-location.

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider.

Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit.

FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unixbased systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.
The following answers are incorrect:
SMTP - Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unixbased systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.
FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available
SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.
The following reference(s) were/was used to create this question: CISA review manual 2014 page number 273 and 274
Topic 7, Malicious Code

NEW QUESTION: 14
Pin, Password, Passphrases, Tokens, smart cards, and biometric devices are all items that can be used for Authentication. When one of these item listed above in conjunction with a second factor to validate authentication, it provides robust authentication of the individual by practicing which of the following?
A. Multi-party authentication
B. Two-factor authentication
C. Mandatory authentication
D. Discretionary authentication
Answer: (SHOW ANSWER)

Once an identity is established it must be authenticated. There exist numerous technologies and implementation of authentication methods however they almost all fall under three major areas.
There are three fundamental types of authentication:
Authentication by knowledge-something a person knows Authentication by possession-something a person has
Authentication by characteristic-something a person is
Logical controls related to these types are called "factors."
Something you know can be a password or PIN, something you have can be a token fob or smart card, and something you are is usually some form of biometrics.
Single-factor authentication is the employment of one of these factors, two-factor authentication is using two of the three factors, and three-factor authentication is the combination of all three factors.
The general term for the use of more than one factor during authentication is multifactor authentication or strong authentication.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 2367-2379). Auerbach Publications. Kindle Edition.

NEW QUESTION: 15
Which of the following is most relevant to determining the maximum effective cost of access control?
A. the value of information that is protected
B. management's perceptions regarding data importance
C. budget planning related to base versus incremental spending.
D. the cost to replace lost data
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The cost of access control must be commensurate with the value of the information that is being protected.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

NEW QUESTION: 16
Which of the following will a Business Impact Analysis NOT identify?
A. Areas that would suffer the greatest financial or operational loss in the event of a disaster.
B. Systems critical to the survival of the enterprise.
C. The names of individuals to be contacted during a disaster.
D. The outage time that can be tolerated by the enterprise as a result of a disaster.
Answer: C (LEAVE A REPLY)
Explanation/Reference:

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 17
The ability to identify and audit a user and his / her actions is known as _____.
A. Accessibility
B. Auditing
C. Forensics
D. Journaling
E. Accountability
Answer: E (LEAVE A REPLY)

NEW QUESTION: 18
Which of the following is an advantage in using a bottom-up versus a top-down approach to software testing?
A. Interface errors are detected earlier.
B. Errors in critical modules are detected earlier.
C. Confidence in the system is achieved earlier.
D. Major functions and processing are tested earlier.
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and work upwards until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices refer to advantages of a top down approach which follows the opposite path.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).

NEW QUESTION: 19
What does the directive of the European Union on Electronic Signatures deal with?

A. Encryption of classified data
B. Encryption of secret data
C. Non repudiation
D. Authentication of web servers
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Reference: FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 589; Directive 1999/93/ EC of 13 December 1999 on a Community framework for electronic signatures.

NEW QUESTION: 20
Examples of types of physical access controls include all EXCEPT which of the following?
A. badges
B. locks
C. guards
D. passwords
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Passwords are considered a Preventive/Technical (logical) control.
The following answers are incorrect:
badges Badges are a physical control used to identify an individual. A badge can include a smart device which can be used for authentication and thus a Technical control, but the actual badge itself is primarily a physical control.
locks Locks are a Preventative Physical control and has no Technical association.
guards Guards are a Preventative Physical control and has no Technical association.
The following reference(s) were/was used to create this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 35).

NEW QUESTION: 21
Instructions or code that executes on an end user's machine from a web browser is known as _____ code.
A. Active X
B. Malware
C. JavaScript
D. Windows Scripting
E. Mobile
Answer: E (LEAVE A REPLY)

NEW QUESTION: 22

Which of the following is used by RADIUS for communication between clients and servers?
A. TCP
B. SSL
C. UDP
D. SSH
Answer: (SHOW ANSWER)
Explanation/Reference:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

NEW QUESTION: 23
Which of the following steps are involved in a basic risk assessment?
A. All of the items listed
B. Determine what data and systems need to be protected
C. Evaluate who are the potential threats
D. Investigate potential legal, financial, and regulatory issues
E. Determine the chances of a disaster or risk related event occurring
F. None of the items listed
Answer: A (LEAVE A REPLY)

NEW QUESTION: 24
Which of the following is not a preventive login control?
A. Last login message
B. Password aging
C. Minimum password length
D. Account expiration
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
The last login message displays the last login date and time, allowing a user to discover if their account was used by someone else. Hence, this is rather a detective control.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 63).

NEW QUESTION: 25
The MOST common threat that impacts a business's ability to function normally is:
A. Power Outage
B. Water Damage
C. Severe Weather
D. Labor Strike
Answer: (SHOW ANSWER)

The MOST common threat that impacts a business's ability to function normally is power. Power interruption cause more business interruption than any other type of event.
The second most common threat is Water such as flood, water damage from broken pipe, leaky roof, etc...
Threats will be discovered while doing your Threats and Risk Assessments (TRA).
There are three elements of risks: threats, assets, and mitigating factors (countermeasures, safeguards, controls).
A threat is an event or situation that if it occured would affect your business and may even prevent it from functioning normally or in some case functioning at all. Evaluation of threats is done by looking at Likelihood and Impact of possible threat. Safeguards, countermeasures, and controls would be used to bring the threat level down to an acceptable level.
Other common events that can impact a company are:
Weather, cable cuts, fires, labor disputes, transportation mishaps, hardware failure, chemical spills, sabotage.
References:
The Official ISC2 Guide to the CISSP CBK, Second Edition, Page 275-276

NEW QUESTION: 26
What can best be described as a domain of trust that shares a single security policy and single management?
A. The reference monitor
B. A security domain
C. The security kernel
D. The security perimeter
Answer: B (LEAVE A REPLY)
A security domain is a domain of trust that shares a single security policy and single management.
The term security domain just builds upon the definition of domain by adding the fact that resources within this logical structure (domain) are working under the same security policy and managed by the same group.
So, a network administrator may put all of the accounting personnel, computers, and network resources in Domain 1 and all of the management personnel, computers, and network resources in Domain 2. These items fall into these individual containers because they not only carry out similar types of business functions, but also, and more importantly, have the same type of trust level. It is this common trust level that allows entities to be managed by one single security policy.
The different domains are separated by logical boundaries, such as firewalls with ACLs, directory services making access decisions, and objects that have their own ACLs indicating which individuals and groups can carry out operations on them.
All of these security mechanisms are examples of components that enforce the security policy for each domain. Domains can be architected in a hierarchical manner that dictates the relationship between the

different domains and the ways in which subjects within the different domains can communicate. Subjects can access resources in domains of equal or lower trust levels.
The following are incorrect answers:
The reference monitor is an abstract machine which must mediate all access to subjects to objects, be protected from modification, be verifiable as correct, and is always invoked. Concept that defines a set of design requirements of a reference validation mechanism (security kernel), which enforces an access control policy over subjects' (processes, users) ability to perform operations (read, write, execute) on objects (files, resources) on a system. The reference monitor components must be small enough to test properly and be tamperproof.
The security kernel is the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept.
The security perimeter includes the security kernel as well as other security-related system functions that are within the boundary of the trusted computing base. System elements that are outside of the security perimeter need not be trusted. not every process and resource falls within the TCB, so some of these components fall outside of an imaginary boundary referred to as the security perimeter. A security perimeter is a boundary that divides the trusted from the untrusted. For the system to stay in a secure and trusted state, precise communication standards must be developed to ensure that when a component within the TCB needs to communicate with a component outside the TCB, the communication cannot expose the system to unexpected security compromises. This type of communication is handled and controlled through interfaces.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 28548-28550). McGraw-Hill. Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 7873-7877). McGraw-Hill. Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition , Access Control, Page 214-217
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Architecture and Design (Kindle Locations 1280-1283). . Kindle Edition.
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
AIO 6th edition chapter 3 access control page 214-217 defines Security domains.
Reference monitor, Security Kernel, and Security Parameter are defined in Chapter 4, Security Architecture and Design.

NEW QUESTION: 27
The Data Encryption Standard (DES) encryption algorithm has which of the following characteristics?
A. 64 bits of data input results in 56 bits of encrypted output
B. 128 bit key with 8 bits used for parity
C. 64 bit blocks with a 64 bit total key length
D. 56 bits of data input results in 56 bits of encrypted output
Answer: (SHOW ANSWER)
Explanation/Reference:

DES works with 64 bit blocks of text using a 64 bit key (with 8 bits used for parity, so the effective key length is 56 bits).
Some people are getting the Key Size and the Block Size mixed up. The block size is usually a specific length. For example DES uses block size of 64 bits which results in 64 bits of encrypted data for each block. AES uses a block size of 128 bits, the block size on AES can only be 128 as per the published standard FIPS-197.
A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte1. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it.
IN CONTRAST WITH AES
The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or
1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits. Other input, output and Cipher Key lengths are not permitted by this standard.
The Advanced Encryption Standard (AES) specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in the AES standard.
The AES algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256".
The other answers are not correct because:
"64 bits of data input results in 56 bits of encrypted output" is incorrect because while DES does work with
64 bit block input, it results in 64 bit blocks of encrypted output.
"128 bit key with 8 bits used for parity" is incorrect because DES does not ever use a 128 bit key.
"56 bits of data input results in 56 bits of encrypted output" is incorrect because DES always works with 64 bit blocks of input/output, not 56 bits.
Reference(s) used for this question:
Official ISC2 Guide to the CISSP CBK, Second Edition, page: 336-343
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

NEW QUESTION: 28
Detective/Technical measures:
A. include intrusion detection systems and automatically-generated violation reports from audit trail information.
B. do not include intrusion detection systems and automatically-generated violation reports from audit trail information.

C. include intrusion detection systems but do not include automatically-generated violation reports from audit trail information.
D. include intrusion detection systems and customised-generated violation reports from audit trail information.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Detective/Technical measures include intrusion detection systems and automatically-generated violation reports from audit trail information. These reports can indicate variations from "normal" operation or detect known signatures of unauthorized access episodes. In order to limit the amount of audit information flagged and reported by automated violation analysis and reporting mechanisms, clipping levels can be set.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

NEW QUESTION: 29
What is the main characteristic of a multi-homed host?
A. It is placed between two routers or firewalls.
B. It allows IP routing.
C. It has multiple network interfaces, each connected to separate networks.
D. It operates at multiple layers.
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The main characteristic of a multi-homed host is that is has multiple network interfaces, each connected to logically and physically separate networks. IP routing should be disabled to prevent the firewall from routing packets directly from one interface to the other.
Source: FERREL, Robert G, Questions and Answers for the CISSP Exam, domain 2 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

NEW QUESTION: 30
This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and access than what is required for the tasks the user needs to fulfill. What best describes this scenario?
A. Excessive Rights
B. Excessive Access
C. Excessive Permissions
D. Excessive Privileges
Answer: D (LEAVE A REPLY)
Even thou all 4 terms are very close to each other, the best choice is Excessive Privileges which would include the other three choices presented.
Reference(s) used for this question:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 645. and

NEW QUESTION: 31
Which of the following choice is NOT normally part of the questions that would be asked in regards to an organization's information security policy?
A. Who is involved in establishing the security policy?
B. Where is the organization's security policy defined?
C. What are the actions that need to be performed in case of a disaster?
D. Who is responsible for monitoring compliance to the organization's security policy?
Answer: C (LEAVE A REPLY)
Actions to be performed in case of a disaster are not normally part of an information security policy but part of a Disaster Recovery Plan (DRP).
Only personnel implicated in the plan should have a copy of the Disaster Recovery Plan whereas everyone should be aware of the contents of the organization's information security policy.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 398).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 32
Which of the following ciphers is a subset on which the Vigenere polyalphabetic cipher was based on?
A. Caesar
B. The Jefferson disks
C. Enigma
D. SIGABA
Answer: A (LEAVE A REPLY)
Explanation/Reference:
In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the Vigenère cipher, and still has modern application in the ROT13 system. As with all single alphabet substitution ciphers, the Caesar cipher is easily broken and in modern practice offers essentially no communication security.
The following answer were incorrect:
The Jefferson disk, or wheel cipher as Thomas Jefferson named it, also known as the Bazeries Cylinder, is a cipher system using a set of wheels or disks, each with the 26 letters of the alphabet arranged around their edge. The order of the letters is different for each disk and is usually scrambled in some random way.
Each disk is marked with a unique number. A hole in the centre of the disks allows them to be stacked on an axle. The disks are removable and can be mounted on the axle in any order desired. The order of the disks is the cipher key, and both sender and receiver must arrange the disks in the same predefined order.
Jefferson's device had 36 disks.
An Enigma machine is any of a family of related electro-mechanical rotor cipher machines used for the encryption and decryption of secret messages. Enigma was invented by the German engineer Arthur Scherbius at the end of World War I. The early models were used commercially from the early 1920s, and adopted by military and government services of several countries. Several different Enigma models were produced, but the German military models are the ones most commonly discussed.
SIGABA: In the history of cryptography, the ECM Mark II was a cipher machine used by the United States for message encryption from World War II until the 1950s. The machine was also known as the SIGABA or Converter M-134 by the Army, or CSP-888/889 by the Navy, and a modified Navy version was termed the CSP-2900. Like many machines of the era it used an electromechanical system of rotors in order to encipher messages, but with a number of security improvements over previous designs. No successful cryptanalysis of the machine during its service lifetime is publicly known.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/Jefferson_disk
http://en.wikipedia.org/wiki/Sigaba
http://en.wikipedia.org/wiki/Enigma_machine

NEW QUESTION: 33
Which of the following statements pertaining to PPTP (Point-to-Point Tunneling Protocol) is incorrect?
A. PPTP allow the tunnelling of any protocols that can be carried within PPP.
B. PPTP does not provide strong encryption.
C. PPTP does not support any token-based authentication method for users.
D. PPTP is derived from L2TP.
Answer: (SHOW ANSWER)
PPTP is an encapsulation protocol based on PPP that works at OSI layer 2 (Data Link) and that enables a single point-to-point connection, usually between a client and a server.
While PPTP depends on IP to establish its connection.

As currently implemented, PPTP encapsulates PPP packets using a modified version of the generic routing encapsulation (GRE) protocol, which gives PPTP to the flexibility of handling protocols other than IP, such as IPX and NETBEUI over IP networks.
PPTP does have some limitations:
It does not provide strong encryption for protecting data, nor does it support any token-based methods for authenticating users.
L2TP is derived from L2F and PPTP, not the opposite.

NEW QUESTION: 34
Which of the following focuses on sustaining an organization's business functions during and after a disruption?
A. Business continuity plan
B. Business recovery plan
C. Continuity of operations plan
D. Disaster recovery plan
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
A business continuity plan (BCP) focuses on sustaining an organization's business functions during and after a disruption. Information systems are considered in the BCP only in terms of their support to the larger business processes. The business recovery plan (BRP) addresses the restoration of business processes after an emergency. The BRP is similar to the BCP, but it typically lacks procedures to ensure continuity of critical processes throughout an emergency or disruption. The continuity of operations plan (COOP) focuses on restoring an organization's essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. The disaster recovery plan (DRP) applies to major, usually catastrophic events that deny access to the normal facility for an extended period. A DRP is narrower in scope than an IT contingency plan in that it does not address minor disruptions that do not require relocation.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page
8).

NEW QUESTION: 35
What can a packet filtering firewall also be called?
A. a scanning router
B. a shielding router
C. a sniffing router
D. a screening router
Answer: (SHOW ANSWER)
Explanation/Reference:

While neither CBK nor AIO3 use the term "screening router," they both discuss how the packet filtering capabilities of a router can be used to block traffic much like a packet filtering firewall. Krutz and Vine use this term on p. 90.
"A scanning router" is incorrect. This is a nonsense term to distract you.
"A shielding router" is incorrect. This is a nonsense term to distract you.
"A sniffing router" is incorrect. This is a nonsense term to distract you.
References:
CBK, p. 433
AIO3, pp.484 - 485

NEW QUESTION: 36
A proxy can control which services (FTP and so on) are used by a workstation , and also aids in protecting the network from outsiders who may be trying to get information about the:
A. network's design
B. user base
C. operating system design
D. net BIOS' design
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
To the untrusted host, all traffic seems to originate from the proxy server and addresses on the trusted network are not revealed.
"User base" is incorrect. The proxy hides the origin of the request from the untrusted host.
"Operating system design" is incorrect. The proxy hides the origin of the request from the untrusted host.
"Net BIOS' design" is incorrect. The proxy hides the origin of the request from the untrusted host.
References:
CBK, p. 467
AIO3, pp. 486 - 490

NEW QUESTION: 37
Which of the following would MOST likely ensure that a system development project meets business objectives?
A. Development and tests are run by different individuals
B. User involvement in system specification and acceptance
C. Development of a project plan identifying all development activities
D. Strict deadlines and budgets
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Effective user involvement is the most critical factor in ensuring that the application meets business objectives.

A great way of getting early input from the user community is by using Prototyping. The prototyping method was formally introduced in the early 1980s to combat the perceived weaknesses of the waterfall model with regard to the speed of development. The objective is to build a simplified version (prototype) of the application, release it for review, and use the feedback from the users' review to build a second, better version.
This is repeated until the users are satisfied with the product. t is a four-step process:
initial concept,
design and implement initial prototype,
refine prototype until acceptable, and
complete and release final version.
There is also the Modified Prototype Model (MPM. This is a form of prototyping that is ideal for Web application development. It allows for the basic functionality of a desired system or component to be formally deployed in a quick time frame. The maintenance phase is set to begin after the deployment. The goal is to have the process be flexible enough so the application is not based on the state of the organization at any given time. As the organization grows and the environment changes, the application evolves with it, rather than being frozen in time.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12101-12108 and 12099-12101). Auerbach Publications. Kindle Edition.
and
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 296).

NEW QUESTION: 38
Which of the following statements pertaining to the security kernel is incorrect?
A. The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept.
B. The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof.
C. The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner.
D. The security kernel is an access control concept, not an actual physical component.
Answer: D (LEAVE A REPLY)
The reference monitor, not the security kernel is an access control concept.
The security kernel is made up of software, and firmware components that fall within the TCB and implements and enforces the reference monitor concept. The security kernel mediates all access and functions between subjects and objects. The security kernel is the core of the TCB and is the most commonly used approach to building trusted computing systems.
There are three main requirements of the security kernel:

It must provide isolation for the processes carrying out the reference monitor concept, and the processes must be tamperproof.
It must be invoked for every access attempt and must be impossible to circumvent. Thus, the security kernel must be implemented in a complete and foolproof way.
It must be small enough to be able to be tested and verified in a complete and comprehensive manner.
The following answers are incorrect:
The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept. Is incorrect because this is the definition of the security kernel.
The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof. Is incorrect because this is one of the three requirements that make up the security kernel.
The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner. Is incorrect because this is one of the three requirements that make up the security kernel.

NEW QUESTION: 39
Which of the following can best define the "revocation request grace period"?
A. The period of time allotted within which the user must make a revocation request upon a revocation reason
B. Minimum response time for performing a revocation by the CA
C. Maximum response time for performing a revocation by the CA
D. Time period between the arrival of a revocation request and the publication of the revocation information
Answer: D (LEAVE A REPLY)
The length of time between the Issuer's receipt of a revocation request and the time the Issuer is required to revoke the certificate should bear a reasonable relationship to the amount of risk the participants are willing to assume that someone may rely on a certificate for which a proper evocation request has been given but has not yet been acted upon.
How quickly revocation requests need to be processed (and CRLs or certificate status databases need to be updated) depends upon the specific application for which the Policy Authority is rafting the Certificate Policy.
A Policy Authority should recognize that there may be risk and lost tradeoffs with respect to grace periods for revocation notices. If the Policy Authority determines that its PKI participants are willing to accept a grace period of a few hours in exchange for a lower implementation cost, the Certificate Policy may reflect that decision.

NEW QUESTION: 40
There are parallels between the trust models in Kerberos and Public Key Infrastructure (PKI). When we compare them side by side, Kerberos tickets correspond most closely to which of the following?
A. public keys

B. private keys
C. public-key certificates
D. private-key certificates
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
A Kerberos ticket is issued by a trusted third party. It is an encrypted data structure that includes the service encryption key. In that sense it is similar to a public-key certificate. However, the ticket is not the key.
The following answers are incorrect:
public keys. Kerberos tickets are not shared out publicly, so they are not like a PKI public key.
private keys. Although a Kerberos ticket is not shared publicly, it is not a private key. Private keys are associated with Asymmetric crypto system which is not used by Kerberos. Kerberos uses only the Symmetric crypto system.
private key certificates. This is a detractor. There is no such thing as a private key certificate.

NEW QUESTION: 41
What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?
A. Central station alarm
B. Proprietary alarm
C. A remote station alarm
D. An auxiliary station alarm
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Auxiliary station alarms automatically cause an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters. They are usually Municipal Fire Alarm Boxes are installed at your business or building, they are wired directly into the fire station.
Central station alarms are operated by private security organizations. It is very similar to a proprietary alarm system (see below). However, the biggest difference is the monitoring and receiving of alarm is done off site at a central location manned by non staff members. It is a third party.
Proprietary alarms are similar to central stations alarms except that monitoring is performed directly on the protected property. This type of alarm is usually use to protect large industrials or commercial buildings. Each of the buildings in the same vincinity has their own alarm system, they are all wired together at a central location within one of the building acting as a common receiving point. This point is usually far away from the other building so it is not under the same danger. It is usually man 24 hours a day by a trained team who knows how to react under different conditions.

A remote station alarm is a direct connection between the signal-initiating device at the protected property and the signal-receiving device located at a remote station, such as the fire station or usually a monitoring service.
This is the most popular type of implementation and the owner of the premise must pay a monthly monitoring fee. This is what most people use in their home where they get a company like ADT to receive the alarms on their behalf.
A remote system differs from an auxiliary system in that it does not use the municipal fire of police alarm circuits.
Reference(s) used for this question:
ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 11: Physical Security (page 211).
and
Great presentation J.T.A. Stone on SlideShare

NEW QUESTION: 42
In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes.
Which of the following would have been true of a Class B network?
A. The first bit of the IP address would be set to zero.
B. The first bit of the IP address would be set to one and the second bit set to zero.
C. The first two bits of the IP address would be set to one, and the third bit set to zero.
D. The first three bits of the IP address would be set to one.
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Each Class B network address has a 16-bit network prefix, with the two highest order bits set to 1-0.
The following answers are incorrect:
The first bit of the IP address would be set to zero. Is incorrect because, this would be a Class A network address.
The first two bits of the IP address would be set to one, and the third bit set to zero. Is incorrect because, this would be a Class C network address.
The first three bits of the IP address would be set to one. Is incorrect because, this is a distractor. Class D & E have the first three bits set to 1. Class D the 4th bit is 0 and for Class E the 4th bit to 1.
Classless Internet Domain Routing (CIDR)
High Order bits are shown in bold below.
For Class A, the addresses are 0.0.0.0 - 127.255.255.255
The lowest Class A address is represented in binary as 00000000.00000000.0000000.00000000 For Class B networks, the addresses are 128.0.0.0 - 191.255.255.255.
The lowest Class B address is represented in binary as 10000000.00000000.00000000.00000000 For Class C, the addresses are 192.0.0.0 - 223.255.255.255 The lowest Class C address is represented in binary as 11000000.00000000.00000000.00000000 For Class D, the addresses are 224.0.0.0 - 239.255.255.255 (Multicast) The lowest Class D address is represented in binary as

11100000.00000000.00000000.00000000 For Class E, the addresses are 240.0.0.0 - 255.255.255.255 (Reserved for future usage) The lowest Class E address is represented in binary as 11110000.00000000.00000000.00000000 Classful IP Address Format
References:
3Com http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf
AIOv3 Telecommunications and Networking Security (page 438)

NEW QUESTION: 43
Which must bear the primary responsibility for determining the level of protection needed for information systems resources?
A. IS security specialists
B. Senior Management
C. Senior security analysts
D. systems Auditors
Answer: B (LEAVE A REPLY)
Explanation/Reference:
If there is no support by senior management to implement, execute, and enforce security policies and procedure, then they won't work. Senior management must be involved in this because they have an obligation to the organization to protect the assests . The requirement here is for management to show "due diligence" in establishing an effective compliance, or security program. It is senior management that could face legal repercussions if they do not have sufficient controls in place.
The following answers are incorrect:
IS security specialists. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.
Senior security analysts. Is incorrect because it is not the best answer. Senior management bears the primary responsibility for determining the level of protection needed.
systems auditors. Is incorrect because it is not the best answer, system auditors are responsible that the controls in place are effective. Senior management bears the primary responsibility for determining the level of protection needed.

NEW QUESTION: 44
Which of the following is NOT a transaction redundancy implementation?
A. on-site mirroring
B. Electronic Vaulting
C. Remote Journaling
D. Database Shadowing
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Three concepts are used to create a level of fault tolerance and redundancy in transaction processing. They are Electronic vaulting, remote journaling and database shadowing provide redundancy at the transaction level.

Electronic vaulting is accomplished by backing up system data over a network. The backup location is usually at a separate geographical location known as the vault site. Vaulting can be used as a mirror or a backup mechanism using the standard incremental or differential backup cycle. Changes to the host system are sent to the vault server in real-time when the backup method is implemented as a mirror. If vaulting updates are recorded in real-time, then it will be necessary to perform regular backups at the off-site location to provide recovery services due to inadvertent or malicious alterations to user or system data.
Journaling or Remote Journaling is another technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location. The journal provides sufficient detail for the transaction to be replayed on the remote system. This provides for database recovery in the event that the database becomes corrupted or unavailable.
There are also additional redundancy options available within application and database software platforms.
For example, database shadowing may be used where a database management system updates records in multiple locations. This technique updates an entire copy of the database at a remote location.
Reference used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20403-20407). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20375-20377). Auerbach Publications. Kindle Edition.

NEW QUESTION: 45
Which of the following security modes of operation involves the highest risk?
A. Compartmented Security Mode
B. Multilevel Security Mode
C. System-High Security Mode
D. Dedicated Security Mode
Answer: (SHOW ANSWER)
In multilevel mode, two or more classification levels of data exist, some people are not cleared for all the data on the system.
Risk is higher because sensitive data could be made available to someone not validated as being capable of maintaining secrecy of that data (i.e., not cleared for it).
In other security modes, all users have the necessary clearance for all data on the system. Source: LaROSA, Jeanette (domain leader), Application and System Development Security CISSP Open Study Guide, version 3.0, January 2002.

NEW QUESTION: 46
What layer of the ISO/OSI model do routers normally operate at?
A. Data link layer

B. Session layer
C. Transport layer
D. Network layer
Answer: (SHOW ANSWER)
Routers are switching devices that operate at the network layer (layer 3) by examining network addresses.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 111).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 47
A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed:
A. at one end of the connection.
B. at both ends of the connection.
C. somewhere between both end points.
D. in the middle of the connection.
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed at both ends of the connection.
In fact it would be a Multiplexer at one end and DeMultiplexer at other end or vice versa. Inverse Multiplexer at both end.
In electronics, a multiplexer (or mux) is a device that selects one of several analog or digital input signals and forwards the selected input into a single line. A multiplexer of 2n inputs has n select lines, which are used to select which input line to send to the output. Multiplexers are mainly used to increase the amount of data that can be sent over the network within a certain amount of time and bandwidth. A multiplexer is also called a data selector.
An electronic multiplexer makes it possible for several signals to share one device or resource, for example one A/D converter or one communication line, instead of having one device per input signal.

On the other hand, a demultiplexer (or demux) is a device taking a single input signal and selecting one of many data-output-lines, which is connected to the single input. A multiplexer is often used with a complementary demultiplexer on the receiving end.
An electronic multiplexer can be considered as a multiple-input, single-output switch, and a demultiplexer as a single-input, multiple-output switch References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.
and
https://secure.wikimedia.org/wikipedia/en/wiki/Multiplexer

NEW QUESTION: 48
Which of the following is defined as the most recent point in time to which data must be synchronized without adversely affecting the organization (financial or operational impacts)?
A. Recovery Point Objective
B. Recovery Time Objective
C. Point of Time Objective
D. Critical Time Objective
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The recovery point objective (RPO) is the maximum acceptable level of data loss following an unplanned "event", like a disaster (natural or man-made), act of crime or terrorism, or any other business or technical disruption that could cause such data loss. The RPO represents the point in time, prior to such an event or incident, to which lost data can be recovered (given the most recent backup copy of the data).
The recovery time objective (RTO) is a period of time within which business and / or technology capabilities must be restored following an unplanned event or disaster. The RTO is a function of the extent to which the interruption disrupts normal operations and the amount of revenue lost per unit of time as a result of the disaster.
These factors in turn depend on the affected equipment and application(s). Both of these numbers represent key targets that are set by key businesses during business continuity and disaster recovery planning; these targets in turn drive the technology and implementation choices for business resumption services, backup / recovery / archival services, and recovery facilities and procedures.
Many organizations put the cart before the horse in selecting and deploying technologies before understanding the business needs as expressed in RPO and RTO; IT departments later bear the brunt of user complaints that their service expectations are not being met. Defining the RPO and RTO can avoid that pitfall, and in doing so can also make for a compelling business case for recovery technology spending and staffing.
For the CISSP candidate studying for the exam, there are no such objectives for "point of time," and "critical time." Those two answers are simply detracters.
Reference:
http://www.wikibon.org/Recovery_point_objective_/_recovery_time_objective_strategy

NEW QUESTION: 49
What is the main characteristic of a multi-homed host?
A. It is placed between two routers or firewalls.
B. It allows IP routing.
C. It has multiple network interfaces, each connected to separate networks.
D. It operates at multiple layers.
Answer: C (LEAVE A REPLY)
The main characteristic of a multi-homed host is that is has multiple network interfaces, each connected to logically and physically separate networks. IP routing should be disabled to prevent the firewall from routing packets directly from one interface to the other.
Source: FERREL, Robert G, Questions and Answers for the CISSP Exam, domain 2 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

NEW QUESTION: 50
In addition to the accuracy of the biometric systems, there are other factors that must also be considered:
A. These factors include the enrollment time and the throughput rate, but not acceptability.
B. These factors do not include the enrollment time, the throughput rate, and acceptability.
C. These factors include the enrollment time, the throughput rate, and acceptability.
D. These factors include the enrollment time, but not the throughput rate, neither the acceptability.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
In addition to the accuracy of the biometric systems, there are other factors that must also be considered. These factors include the enrollment time, the throughput rate, and acceptability.
Enrollment time is the time it takes to initially "register" with a system by providing samples of the biometric characteristic to be evaluated. An acceptable enrollment time is around two minutes.
For example, in fingerprint systems, the actual fingerprint is stored and requires approximately 250kb per finger for a high quality image. This level of information is required for one-to-many searches in forensics applications on very large databases.
In finger-scan technology, a full fingerprint is not stored-the features extracted from this fingerprint are stored using a small template that requires approximately 500 to 1000 bytes of storage. The original fingerprint cannot be reconstructed from this template.
Updates of the enrollment information may be required because some biometric characteristics, such as voice and signature, may change with time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37 & 38.

NEW QUESTION: 51
Which protocol is used to send email?
A. File Transfer Protocol (FTP).
B. Post Office Protocol (POP).

C. Network File System (NFS).
D. Simple Mail Transfer Protocol (SMTP).
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. POP is a protocol used to retrieve e-mail from a mail server. NFS is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture. FTP is the protocol that is used to facilitate file transfer between two machines.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

NEW QUESTION: 52
Complete the blanks. When using PKI, I digitally sign a message using my _____ key. The recipient verifies my signature using my _____ key.
A. Private / Public
B. Public / Private
C. Symmetric / Asymmetric
D. Private / Symmetric
Answer: A (LEAVE A REPLY)
Explanation/Reference:
When we encrypt messages using our private keys which are only available to us. The person who wants to read and decrypt the message need only have our public keys to do so.
The whole point to PKI is to assure message integrity, authentication of the source, and to provide secrecy with the digital encryption.
See below a nice walktrough of Digital Signature creation and verification from the Comodo web site:
Digital Signatures apply the same functionality to an e-mail message or data file that a handwritten signature does for a paper-based document. The Digital Signature vouches for the origin and integrity of a message, document or other data file.
How do we create a Digital Signature?
The creation of a Digital Signature is a complex mathematical process. However as the complexities of the process are computed by the computer, applying a Digital Signature is no more difficult that creating a handwritten one!
The following text illustrates in general terms the processes behind the generation of a Digital Signature:
1. Alice clicks 'sign' in her email application or selects which file is to be signed.
2. Alice's computer calculates the 'hash' (the message is applied to a publicly known mathematical hashing function that coverts the message into a long number referred to as the hash).
3. The hash is encrypted with Alice's Private Key (in this case it is known as the Signing Key) to create the Digital Signature.
4. The original message and its Digital Signature are transmitted to Bob.

5. Bob receives the signed message. It is identified as being signed, so his email application knows which actions need to be performed to verify it.
6. Bob's computer decrypts the Digital Signature using Alice's Public Key.
7. Bob's computer also calculates the hash of the original message (remember - the mathematical function used by Alice to do this is publicly known).
8. Bob's computer compares the hashes it has computed from the received message with the now decrypted hash received with Alice's message.
digital signature creation and verification
If the message has remained integral during its transit (i.e. it has not been tampered with), when compared the two hashes will be identical.
However, if the two hashes differ when compared then the integrity of the original message has been compromised. If the original message is tampered with it will result in Bob's computer calculating a different hash value. If a different hash value is created, then the original message will have been altered. As a result the verification of the Digital Signature will fail and Bob will be informed.
Origin, Integrity, Non-Repudiation, and Preventing Men-In-The-Middle (MITM) attacks Eve, who wants to impersonate Alice, cannot generate the same signature as Alice because she does not have Alice's Private Key (needed to sign the message digest). If instead, Eve decides to alter the content of the message while in transit, the tampered message will create a different message digest to the original message, and Bob's computer will be able to detect that. Additionally, Alice cannot deny sending the message as it has been signed using her Private Key, thus ensuring non-repudiation.
creating and validating a digital signature
Due to the recent Global adoption of Digital Signature law, Alice may now sign a transaction, message or piece of digital data, and so long as it is verified successfully it is a legally permissible means of proof that Alice has made the transaction or written the message.
The following answers are incorrect:
- Public / Private: This is the opposite of the right answer.
- Symmetric / Asymmetric: Not quite. Sorry. This form of crypto is asymmetric so you were almost on target.
- Private / Symmetric: Well, you got half of it right but Symmetric is wrong.
The following reference(s) was used to create this question:
The CCCure Holistic Security+ CBT, you can subscribe at: http://www.cccure.tv and http://www.comodo.com/resources/small-business/digital-certificates3.php

NEW QUESTION: 53
When a biometric system is used, which error type deals with the possibility of GRANTING access to impostors who should be REJECTED?
A. Type I error
B. Type II error
C. Type III error
D. Crossover error
Answer: B (LEAVE A REPLY)

Section: Access Control
Explanation/Reference:
When the biometric system accepts impostors who should have been rejected , it is called a Type II error or False Acceptance Rate or False Accept Rate.
Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of verifying identification.
Biometrics is a very sophisticated technology; thus, it is much more expensive and complex than the other types of identity verification processes. A biometric system can make authentication decisions based on an individual's behavior, as in signature dynamics, but these can change over time and possibly be forged.
Biometric systems that base authentication decisions on physical attributes (iris, retina, fingerprint) provide more accuracy, because physical attributes typically don't change much, absent some disfiguring injury, and are harder to impersonate.
When a biometric system rejects an authorized individual, it is called a Type I error (False Rejection Rate (FRR) or False Reject Rate (FRR)).
When the system accepts impostors who should be rejected, it is called a Type II error (False Acceptance Rate (FAR) or False Accept Rate (FAR)). Type II errors are the most dangerous and thus the most important to avoid.
The goal is to obtain low numbers for each type of error, but When comparing different biometric systems, many different variables are used, but one of the most important metrics is the crossover error rate (CER).
The accuracy of any biometric method is measured in terms of Failed Acceptance Rate (FAR) and Failed Rejection Rate (FRR). Both are expressed as percentages. The FAR is the rate at which attempts by unauthorized users are incorrectly accepted as valid. The FRR is just the opposite. It measures the rate at which authorized users are denied access.
The relationship between FRR (Type I) and FAR (Type II) is depicted in the graphic below . As one rate increases, the other decreases. The Cross-over Error Rate (CER) is sometimes considered a good indicator of the overall accuracy of a biometric system. This is the point at which the FRR and the FAR have the same value. Solutions with a lower CER are typically more accurate.
See graphic below from Biometria showing this relationship. The Cross-over Error Rate (CER) is also called the Equal Error Rate (EER), the two are synonymous.
Cross Over Error Rate
The other answers are incorrect:
Type I error is also called as False Rejection Rate where a valid user is rejected by the system.
Type III error : there is no such error type in biometric system.
Crossover error rate stated in percentage , represents the point at which false rejection equals the false acceptance rate.
Reference(s) used for this question:
http://www.biometria.sk/en/principles-of-biometrics.html
and

Shon Harris, CISSP All In One (AIO), 6th Edition , Chapter 3, Access Control, Page 188-189 and Tech Republic, Reduce Multi_Factor Authentication Cost

NEW QUESTION: 54
Which of the following biometric devices offers the LOWEST CER?
A. Keystroke dynamics
B. Voice verification
C. Iris scan
D. Fingerprint
Answer: C (LEAVE A REPLY)
Explanation/Reference:
From most effective (lowest CER) to least effective (highest CER) are:
Iris scan, fingerprint, voice verification, keystroke dynamics.
Reference : Shon Harris Aio v3 , Chapter-4 : Access Control , Page : 131 Also see:
http://www.sans.org/reading_room/whitepapers/authentication/biometric-selection-body-parts- online_139

NEW QUESTION: 55
Which of the following cannot be undertaken in conjunction or while computer incident handling is ongoing?
A. System development activity
B. Help-desk function
C. System Imaging
D. Risk management process
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
If Incident Handling is underway an incident has potentially been identified. At that point all use of the system should stop because the system can no longer be trusted and any changes could contaminate the evidence.
This would include all System Development Activity.
Every organization should have plans and procedures in place that deals with Incident Handling. Employees should be instructed what steps are to be taken as soon as an incident occurs and how to report it.
It is important that all parties involved are aware of these steps to protect not only any possible evidence but also to prevent any additional harm.
It is quite possible that the fraudster has planted malicous code that could cause destruction or even a Trojan Horse with a back door into the system. As soon as an incident has been identified the system can no longer be trusted and all use of the system should cease.
Shon Harris in her latest book mentions:
Although we commonly use the terms "event" and "incident" interchangeably, there are subtle differences between the two. An event is a negative occurrence that can be observed, verified, and documented,

whereas an incident is a series of events that negatively affects the company and/ or impacts its security posture. This is why we call reacting to these issues "incident response" (or "incident handling"), because something is negatively affecting the company and causing a security breach.

Many types of incidents (virus, insider attack, terrorist attacks, and so on) exist, and sometimes it is just human error. Indeed, many incident response individuals have received a frantic call in the middle of the night because a system is acting "weird." The reasons could be that a deployed patch broke something, someone misconfigured a device, or the administrator just learned a new scripting language and rolled out some code that caused mayhem and confusion.

When a company endures a computer crime, it should leave the environment and evidence unaltered and contact whomever has been delegated to investigate these types of situations. Someone who is unfamiliar with the proper process of collecting data and evidence from a crime scene could instead destroy that evidence, and thus all hope of prosecuting individuals, and achieving a conviction would be lost.

Companies should have procedures for many issues in computer security such as enforcement procedures, disaster recovery and continuity procedures, and backup procedures. It is also necessary to have a procedure for dealing with computer incidents because they have become an increasingly important issue of today's information security departments. This is a direct result of attacks against networks and information systems increasing annually. Even though we don't have specific numbers due to a lack of universal reporting and reporting in general, it is clear that the volume of attacks is increasing. Just think about all the spam, phishing scams, malware, distributed denial-of-service, and other attacks you see on your own network and hear about in the news. Unfortunately, many companies are at a loss as to who to call or what to do right after they have been the victim of a cybercrime. Therefore, all companies should have an incident response policy that indicates who has the authority to initiate an incident response, with supporting procedures set up before an incident takes place.

This policy should be managed by the legal department and security department. They need to work together to make sure the technical security issues are covered and the legal issues that surround criminal activities are properly dealt with. The incident response policy should be clear and concise. For example, it should indicate if systems can be taken offline to try to save evidence or if systems have to continue functioning at the risk of destroying evidence. Each system and functionality should have a priority assigned to it. For instance, if the file server is infected, it should be removed from the network, but not shut down. However, if the mail server is infected, it should not be removed from the network or shut down because of the priority the company attributes to the mail server over the file server. Tradeoffs and decisions will have to be made, but it is better to think through these issues before the situation occurs, because better logic is usually possible before a crisis, when there's less emotion and chaos.

The Australian Computer Emergency Response Team's General Guidelines for Computer Forensics:

Keep the handling and corruption of original data to a minimum.

Document all actions and explain changes.

Follow the Five Rules for Evidence (Admissible, Authentic, Complete, Accurate, Convincing).

* Bring in more experienced help when handling and/ or analyzing the evidence is beyond your knowledge, skills, or abilities.

Adhere to your organization's security policy and obtain written permission to conduct a forensics investigation.
Capture as accurate an image of the system(s) as possible while working quickly.
Be ready to testify in a court of law.
Make certain your actions are repeatable.
Prioritize your actions, beginning with volatile and proceeding to persistent evidence.
Do not run any programs on the system(s) that are potential evidence.
Act ethically and in good faith while conducting a forensics investigation, and do not attempt to do any harm.
The following answers are incorrect:
help-desk function. Is incorrect because during an incident, employees need to be able to communicate with a central source. It is most likely that would be the help-desk. Also the help-desk would need to be able to communicate with the employees to keep them informed.
system imaging. Is incorrect because once an incident has occured you should perform a capture of evidence starting with the most volatile data and imaging would be doen using bit for bit copy of storage medias to protect the evidence.
risk management process. Is incorrect because incident handling is part of risk management, and should continue.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21468-21476). McGraw-Hill. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21096-21121). McGraw-Hill. Kindle Edition.
and
NIST Computer Security incident handling http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter12.html

NEW QUESTION: 56
Which of the following answers is described as a random value used in cryptographic algorithms to ensure that patterns are not created during the encryption process?
A. IV - Initialization Vector
B. Stream Cipher
C. OTP - One Time Pad
D. Ciphertext
Answer: A (LEAVE A REPLY)
The basic power in cryptography is randomness. This uncertainty is why encrypted data is unusable to someone without the key to decrypt.
Initialization Vectors are a used with encryption keys to add an extra layer of randomness to encrypted data. If no IV is used the attacker can possibly break the keyspace because of patterns resulting in the

encryption process. Implementation such as DES in Code Book Mode (CBC) would allow frequency analysis attack to take place.
In cryptography, an initialization vector (IV) or starting variable (SV)is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom.
Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by so-called modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.
It is define by TechTarget as:
An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.
The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding sequences in the message were also identical. The IV prevents the appearance of corresponding duplicate character sequences in the ciphertext.
The following answers are incorrect:
-Stream Cipher: This isn't correct. A stream cipher is a symmetric key cipher where plaintext digits are combined with pseudorandom key stream to product cipher text.
-OTP - One Time Pad: This isn't correct but OTP is made up of random values used as key material. (Encryption key) It is considered by most to be unbreakable but must be changed with a new key after it is used which makes it impractical for common use.
-Ciphertext: Sorry, incorrect answer. Ciphertext is basically text that has been encrypted with key material (Encryption key)
The following reference(s) was used to create this question:
For more details on this TOPIC and other questions of the Security+ CBK, subscribe to our Holistic Computer Based Tutorial (CBT) at http://www.cccure.tv and whatis.techtarget.com/definition/initialization-vector-IV and en.wikipedia.org/wiki/Initialization_vector

NEW QUESTION: 57
Which layer of the DoD TCP/IP model controls the communication flow between hosts?
A. Internet layer
B. Host-to-host transport layer
C. Application layer
D. Network access layer
Answer: B (LEAVE A REPLY)
Explanation/Reference:

Whereas the host-to-host layer (equivalent to the OSI's transport layer) provides end-to-end data delivery service, flow control, to the application layer.
The four layers in the DoD model, from top to bottom, are:
The Application Layer contains protocols that implement user-level functions, such as mail delivery, file transfer and remote login.
The Host-to-Host Layer handles connection rendez vous, flow control, retransmission of lost data, and other generic data flow management between hosts. The mutually exclusive TCP and UDP protocols are this layer's most important members.
The Internet Layer is responsible for delivering data across a series of different physical networks that interconnect a source and destination machine. Routing protocols are most closely associated with this layer, as is the IP Protocol, the Internet's fundamental protocol.
The Network Access Layer is responsible for delivering data over the particular hardware media in use. Different protocols are selected from this layer, depending on the type of physical network The OSI model organizes communication services into seven groups called layers. The layers are as follows:
Layer 7, The Application Layer: The application layer serves as a window for users and application processes to access network services. It handles issues such as network transparency, resource allocation, etc. This layer is not an application in itself, although some applications may perform application layer functions.
Layer 6, The Presentation Layer: The presentation layer serves as the data translator for a network. It is usually a part of an operating system and converts incoming and outgoing data from one presentation format to another. This layer is also known as syntax layer.
Layer 5, The Session Layer: The session layer establishes a communication session between processes running on different communication entities in a network and can support a message-mode data transfer. It deals with session and connection coordination.
Layer 4, The Transport Layer: The transport layer ensures that messages are delivered in the order in which they are sent and that there is no loss or duplication. It ensures complete data transfer. This layer provides an additional connection below the Session layer and assists with managing some data flow control between hosts. Data is divided into packets on the sending node, and the receiving node's Transport layer reassembles the message from packets. This layer is also responsible for error checking to guarantee error-free data delivery, and requests a retransmission if necessary. It is also responsible for sending acknowledgments of successful transmissions back to the sending host. A number of protocols run at the Transport layer, including TCP, UDP, Sequenced Packet Exchange (SPX), and NWLink.
Layer 3, The Network Layer: The network layer controls the operation of the subnet. It determines the physical path that data takes on the basis of network conditions, priority of service, and other factors. The network layer is responsible for routing and forwarding data packets.
Layer 2, The Data-Link Layer: The data-link layer is responsible for error free transfer of data frames. This layer provides synchronization for the physical layer. ARP and RARP would be found at this layer.
Layer 1, The Physical Layer: The physical layer is responsible for packaging and transmitting data on the physical media. This layer conveys the bit stream through a network at the electrical and mechanical level.
See a great flash animation on the subject at:

http://www.maris.com/content/applets/flash/comp/fa0301.swf
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
85).
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7:
Telecommunications and Network Security (page 344).

NEW QUESTION: 58
Which of the following statements pertaining to software testing is incorrect?
A. Unit testing should be addressed and considered when the modules are being designed.
B. Test data should be part of the specifications.
C. Testing should be performed with live data to cover all possible situations.
D. Test data generators can be used to systematically generate random test data that can be used to test programs.
Answer: (SHOW ANSWER)
Explanation/Reference:
Live or actual field data is not recommended for use in the testing procedures because both data types may not cover out of range situations and the correct outputs of the test are unknown. Live data would not be the best data to use because of the lack of anomalies and also because of the risk of exposure to your live data.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 251).

NEW QUESTION: 59
Which one of the following is usually not a benefit resulting from the use of firewalls?
A. reduces the risks of external threats from malicious hackers.
B. prevents the spread of viruses.
C. reduces the threat level on internal system.
D. allows centralized management and control of services.
Answer: B (LEAVE A REPLY)
This is not a benefit of a firewall. Most firewalls are limited when it comes to preventing the spread of viruses.
This question is testing your knowledge of Malware and Firewalls. The keywords within the questions are "usually" and "virus". Once again to come up with the correct answer, you must stay within the context of the question and really ask yourself which of the 4 choices is NOT usually done by a firewall.
Some of the latest Appliances such as Unified Threat Management (UTM) devices does have the ability to do virus scanning but most first and second generation firewalls would not have such ability.

Remember, the questions is not asking about all possible scenarios that could exist but only about which of the 4 choices presented is the BEST.
For the exam you must know your general classes of Malware. There are generally four major classes of malicious code that fall under the general definition of malware:
1.Virus: Parasitic code that requires human action or insertion, or which attaches itself to another program to facilitate replication and distribution. Virus-infected containers can range from e-mail, documents, and data file macros to boot sectors, partitions, and memory fobs. Viruses were the first iteration of malware and were typically transferred by floppy disks (also known as "sneakernet") and injected into memory when the disk was accessed or infected files were transferred from system to system.
2.Worm: Self-propagating code that exploits system or application vulnerabilities to replicate. Once on a system, it may execute embedded routines to alter, destroy, or monitor the system on which it is running, then move on to the next system. A worm is effectively a virus that does not require human interaction or other programs to infect systems.
3.Trojan Horse: Named after the Trojan horse of Greek mythology (and serving a very similar function), a Trojan horse is a general term referring to programs that appear desirable, but actually contain something harmful. A Trojan horse purports to do one thing that the user wants while secretly performing other potentially malicious actions. For example, a user may download a game file, install it, and begin playing the game. Unbeknownst to the user, the application may also install a virus, launch a worm, or install a utility allowing an attacker to gain unauthorized access to the system remotely, all without the user's knowledge.
4.Spyware: Prior to its use in malicious activity, spyware was typically a hidden application injected through poor browser security by companies seeking to gain more information about a user's Internet activity. Today, those methods are used to deploy other malware, collect private data, send advertising or commercial messages to a system, or monitor system input, such as keystrokes or mouse clicks.
The following answers are incorrect:
reduces the risks of external threats from malicious hackers. This is incorrect because a firewall can reduce the risks of external threats from malicious hackers.
reduces the threat level on internal system. This is incorrect because a firewall can reduce the threat level on internal system.
allows centralized management and control of services. This is incorrect because a firewall can allow centralize management and control of services.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3989-4009). Auerbach Publications. Kindle Edition.

NEW QUESTION: 60
An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):
A. active attack
B. outside attack

C. inside attack
D. passive attack
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
An inside attack is an attack initiated by an entity inside the security perimeter, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization whereas an outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system. An active attack attempts to alter system resources to affect their operation and a passive attack attempts to learn or make use of the information from the system but does not affect system resources.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 61
What is called the type of access control where there are pairs of elements that have the least upper bound of values and greatest lower bound of values?
A. Mandatory model
B. Discretionary model
C. Lattice model
D. Rule model
Answer: C (LEAVE A REPLY)
Explanation/Reference:
In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 62
How many bits of a MAC address uniquely identify a vendor, as provided by the IEEE?
A. 6 bits
B. 12 bits

C. 16 bits
D. 24 bits
Answer: D (LEAVE A REPLY)
Explanation/Reference:
The MAC address is 48 bits long, 24 of which identify the vendor, as provided by the IEEE. The other 24 bits are provided by the vendor.
A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.
MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This is can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address. An example is many SOHO routers, where the ISP grants access to only one MAC address (used previously to inserting the router) so the router must use that MAC address on its Internet-facing NIC. Therefore the router administrator configures a MAC address to override the burned-in one.
A network node may have multiple NICs and each must have one unique MAC address per NIC.
See diagram below from Wikipedia showing the format of a MAC address. :
MAC Address format
Reference(s) used for this question:
http://en.wikipedia.org/wiki/MAC_address

NEW QUESTION: 63
Making sure that only those who are supposed to access the data can access is which of the following?
A. confidentiality.
B. capability.
C. integrity.
D. availability.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
From the published (ISC)2 goals for the Certified Information Systems Security Professional candidate, domain definition. Confidentiality is making sure that only those who are supposed to access the data can access it.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 64
Which conceptual approach to intrusion detection system is the most common?

A. Behavior-based intrusion detection
B. Knowledge-based intrusion detection
C. Statistical anomaly-based intrusion detection
D. Host-based intrusion detection
Answer: (SHOW ANSWER)
Explanation/Reference:
There are two conceptual approaches to intrusion detection. Knowledge-based intrusion detection uses a database of known vulnerabilities to look for current attempts to exploit them on a system and trigger an alarm if an attempt is found. The other approach, not as common, is called behaviour-based or statistical analysis-based. A host-based intrusion detection system is a common implementation of intrusion detection, not a conceptual approach.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
63).
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4:
Access Control (pages 193-194).

NEW QUESTION: 65
Which of the following questions is less likely to help in assessing an organization's contingency planning controls?
A. Is damaged media stored and/or destroyed?
B. Are the backup storage site and alternate site geographically far enough from the primary site?
C. Is there an up-to-date copy of the plan stored securely off-site?
D. Is the location of stored backups identified?
Answer: A (LEAVE A REPLY)
Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small.
Handling of damaged media is an operational task related to regular production and is not specific to contingency planning. Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-27 to A-28).

NEW QUESTION: 66
Which of the following backup methods makes a complete backup of every file on the server every time it is run?
A. full backup method.
B. incremental backup method.
C. differential backup method.
D. tape backup method.

Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
The Full Backup Method makes a complete backup of every file on the server every time it is run.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

NEW QUESTION: 67
Which one of the following statements about the advantages and disadvantages of network-based Intrusion detection systems is true
A. Network-based IDSs are not vulnerable to attacks.
B. Network-based IDSs are well suited for modern switch-based networks.
C. Most network-based IDSs can automatically indicate whether or not an attack was successful.
D. The deployment of network-based IDSs has little impact upon an existing network.
Answer: (SHOW ANSWER)
Section: Analysis and Monitoring
Explanation/Reference:
Network-based IDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a network. Thus, it is usually easy to retrofit a network to include network-based IDSs with minimal effort.
Network-based IDSs are not vulnerable to attacks is not true, even thou network-based IDSs can be made very secure against attack and even made invisible to many attackers they still have to read the packets and sometimes a well crafted packet might exploit or kill your capture engine.
Network-based IDSs are well suited for modern switch-based networks is not true as most switches do not provide universal monitoring ports and this limits the monitoring range of a network-based IDS sensor to a single host. Even when switches provide such monitoring ports, often the single port cannot mirror all traffic traversing the switch.
Most network-based IDSs can automatically indicate whether or not an attack was successful is not true as most network-based IDSs cannot tell whether or not an attack was successful; they can only discern that an attack was initiated. This means that after a network-based IDS detects an attack, administrators must manually investigate each attacked host to determine whether it was indeed penetrated.
Reference:
NIST special publication 800-31 Intrusion Detection System pages 15-16
Official guide to the CISSP CBK. Pages 196 to 197

NEW QUESTION: 68
The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit is called:
A. alteration
B. investigation

C. entrapment
D. enticement.
Answer: D (LEAVE A REPLY)
Enticement deals with someone that is breaking the law. Entrapment encourages someone to commit a crime that the individual may or many have had no intention of committing. Enticement is not necessarily illegal but does raise ethical arguments and may not be admissible in court. Enticement lures someone toward some evidence (a honeypot would be a great example) after that individual has already committed a crime.
Entrapment is when you persuade someone to commit a crime when the person otherwise had no intention to commit a crime. Entrapment is committed by a law enforcement player where you get tricked into committing a crime for which you woud later on get arrested without knowing you rare committing such a scrime. It is illegal and unethical as well.
All other choices were not applicable and only detractors.
References:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation. and CISSP Study Guide (Conrad, Misenar, Feldman). Elsevier. 2010. p. 428 and http://www.dummies.com/how-to/content/security-certification-computer-forensics-andinci.html

NEW QUESTION: 69
Of the reasons why a Disaster Recovery plan gets outdated, which of the following is not true?
A. Personnel turnover
B. Large plans can take a lot of work to maintain
C. Continous auditing makes a Disaster Recovery plan irrelevant
D. Infrastructure and environment changes
Answer: C (LEAVE A REPLY)
Although a auditing is a part of corporate security, it in no way supercedes the requirments for a disaster recovery plan. All others can be blamed for a plan going out of date. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 609).

NEW QUESTION: 70
Which of the following service is a distributed database that translate host name to IP address to IP address to host name?
A. DNS
B. FTP
C. SSH
D. SMTP
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names

with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

For your exam you should know below information general Internet terminology:

Network access point - Internet service providers access internet using net access point.A Network Access Point (NAP) was a public network exchange facility where Internet service providers (ISPs) connected with one another in peering arrangements. The NAPs were a key component in the transition from the 1990s NSFNET era (when many networks were government sponsored and commercial traffic was prohibited) to the commercial Internet providers of today. They were often points of considerable Internet congestion.

Internet Service Provider (ISP) - An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, co-location.

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider.

Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer.

It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/ server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow

anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available
Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.
The following answers are incorrect:
SMTP - Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.
On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.
FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available
SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, ssh, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 273 and 274

NEW QUESTION: 71
What type of attack involves IP spoofing, ICMP ECHO and a bounce site?
A. IP spoofing attack
B. Teardrop attack
C. SYN attack
D. Smurf attack
Answer: (SHOW ANSWER)

Explanation/Reference:
A smurf attack occurs when an attacker sends a spoofed (IP spoofing) PING (ICMP ECHO) packet to the broadcast address of a large network (the bounce site). The modified packet containing the address of the target system, all devices on its local network respond with a ICMP REPLY to the target system, which is then saturated with those replies. An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A teardrop attack consists of modifying the length and fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
76).

NEW QUESTION: 72
In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class B network?
A. The first bit of the IP address would be set to zero.
B. The first bit of the IP address would be set to one and the second bit set to zero.
C. The first two bits of the IP address would be set to one, and the third bit set to zero.
D. The first three bits of the IP address would be set to one.
Answer: (SHOW ANSWER)
Each Class B network address has a 16-bit network prefix, with the two highest order bits set to 1-0.
The following answers are incorrect:
The first bit of the IP address would be set to zero. Is incorrect because, this would be a Class A network address.
The first two bits of the IP address would be set to one, and the third bit set to zero. Is incorrect because, this would be a Class C network address.
The first three bits of the IP address would be set to one. Is incorrect because, this is a distractor. Class D & E have the first three bits set to 1. Class D the 4th bit is 0 and for Class E the 4th bit to 1.
Classless Internet Domain Routing (CIDR) High Order bits are shown in bold below.
For Class A, the addresses are 0.0.0.0 - 127.255.255.255 The lowest Class A address is represented in binary as 00000000.00000000.0000000.00000000
For Class B networks, the addresses are 128.0.0.0 - 191.255.255.255. The lowest Class B address is represented in binary as 10000000.00000000.00000000.00000000
For Class C, the addresses are 192.0.0.0 - 223.255.255.255 The lowest Class C address is represented in binary as 11000000.00000000.00000000.00000000
For Class D, the addresses are 224.0.0.0 - 239.255.255.255 (Multicast) The lowest Class D address is represented in binary as 11100000.00000000.00000000.00000000

For Class E, the addresses are 240.0.0.0 - 255.255.255.255 (Reserved for future usage) The lowest Class E address is represented in binary as 11110000.00000000.00000000.00000000 Classful IP Address Format
References: 3Com http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf
AIOv3 Telecommunications and Networking Security (page 438)

NEW QUESTION: 73
A DMZ is also known as a
A. screened subnet
B. three legged firewall
C. a place to attract hackers
D. bastion host
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
This is another name for the demilitarized zone (DMZ) of a network.
"Three legged firewall" is incorrect. While a DMZ can be implemented on one leg of such a device, this is not the best answer.
"A place to attract hackers" is incorrect. The DMZ is a way to provide limited public access to an organization's internal resources (DNS, EMAIL, public web, etc) not as an attractant for hackers.
"Bastion host" is incorrect. A bastion host serves as a gateway between trusted and untrusted network.
References:
CBK, p. 434
AIO3, pp. 495 - 496

NEW QUESTION: 74
What is the most critical characteristic of a biometric identifying system?
A. Perceived intrusiveness
B. Storage requirements
C. Accuracy
D. Scalability
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Accuracy is the most critical characteristic of a biometric identifying verification system.
Accuracy is measured in terms of false rejection rate (FRR, or type I errors) and false acceptance rate (FAR or type II errors).
The Crossover Error Rate (CER) is the point at which the FRR equals the FAR and has become the most important measure of biometric system accuracy.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 9).

NEW QUESTION: 75
The Crossover Error Rate (CER) is a good measure of performance for:
A. Biometrics
B. Tokens
C. Kerberos
D. A fingerprint scan
E. Discretionary access control
Answer: A (LEAVE A REPLY)
The CER is one of the three main performance measurements used in biometrics.

NEW QUESTION: 76
What IDS approach relies on a database of known attacks?
A. Signature-based intrusion detection
B. Statistical anomaly-based intrusion detection
C. Behavior-based intrusion detection
D. Network-based intrusion detection
Answer: A (LEAVE A REPLY)
A weakness of the signature-based (or knowledge-based) intrusion detection approach is that only attack signatures that are stored in a database are detected. Network-based intrusion detection can either be signature-based or statistical anomaly-
based (also called behavior-based).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 49).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 77
The Terminal Access Controller Access Control System (TACACS) employs which of the following?
A. a user ID and static password for network access
B. a user ID and dynamic password for network access
C. a user ID and symmetric password for network access
D. a user ID and asymmetric password for network access

Answer: A (LEAVE A REPLY)

Explanation/Reference:

For networked applications, the Terminal Access Controller Access Control System (TACACS) employs a user ID and a static password for network access.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 44.

NEW QUESTION: 78

Which of the following statements pertaining to Secure Sockets Layer (SSL) is false?

A. The SSL protocol was developed by Netscape to secure Internet client-server transactions.

B. The SSL protocol's primary use is to authenticate the client to the server using public key cryptography and digital certificates.

C. Web pages using the SSL protocol start with HTTPS

D. SSL can be used with applications such as Telnet, FTP and email protocols.

Answer: (SHOW ANSWER)

All of these statements pertaining to SSL are true except that it is primary use is to authenticate the client to the server using public key cryptography and digital certificates. It is the opposite, Its primary use is to authenticate the server to the client.

The following reference(s) were used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 170).

NEW QUESTION: 79

Which of the following is NOT an administrative control?

A. Logical access control mechanisms

B. Screening of personnel

C. Development of policies, standards, procedures and guidelines

D. Change control procedures

Answer: (SHOW ANSWER)

Explanation/Reference:

It is considered to be a technical control.

Logical is synonymous with Technical Control. That was the easy answer.

There are three broad categories of access control: Administrative, Technical, and Physical. Each category has different access control mechanisms that can be carried out manually or automatically.

All of these access control mechanisms should work in concert with each other to protect an infrastructure and its data.

Each category of access control has several components that fall within it, as shown here:

Administrative Controls

* Policy and procedures

* Personnel controls
* Supervisory structure
* Security-awareness training
* Testing
Physical Controls
Network segregation
Perimeter security
Computer controls
Work area separation
Data backups
Technical Controls
System access
Network architecture
Network access
Encryption and protocols
Control zone
Auditing
The following answers are incorrect :
Screening of personnel is considered to be an administrative control
Development of policies, standards, procedures and guidelines is considered to be an administrative control
Change control procedures is considered to be an administrative control.
Reference : Shon Harris AIO v3 , Chapter - 3 : Security Management Practices , Page : 52-54

NEW QUESTION: 80
Which OSI/ISO layer is responsible for determining the best route for data to be transferred?
A. Session layer
B. Physical layer
C. Network layer
D. Transport layer
Answer: C (LEAVE A REPLY)
Explanation/Reference:
The main responsibility of the network layer is to insert information into the packet's header so that it can be properly routed. The protocols at the network layer must determine the best path for the packet to take.
The following answers are incorrect:
Session layer. The session layer is responsible for establishing a connection between two applications.
Physical layer. The physical layer if responsible for converting electronic impulses into bits and vice-versa.
Transport layer. The transport layer is responsible for data transmission and error detection.
The following reference(s) were/was used to create this question:

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, v3, chapter 7:
Telecommunications and Network Security (page 422-428).
ISC2 Official ISC2 Guide to the CBK (OIG) 2007, p. 409-412

NEW QUESTION: 81
Domain Name Service is a distributed database system that is used to map:
A. Domain Name to IP addresses.
B. MAC addresses to domain names.
C. MAC Address to IP addresses.
D. IP addresses to MAC Addresses.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The Domain Name Service is a distributed database system that is used to map domain names to IP addresses and IP addresses to domain names.
The Domain Name System is maintained by a distributed database system, which uses the client-server model. The nodes of this database are the name servers. Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root nameservers, the servers to query when looking up (resolving) a TLD.
Reference(s) used for this question:
KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100.
and
https://en.wikipedia.org/wiki/Domain_Name_System

NEW QUESTION: 82
Which of the following are the steps usually followed in the development of documents such as security policy, standards and procedures?
A. design, development, publication, coding, and testing.
B. design, evaluation, approval, publication, and implementation.
C. initiation, evaluation, development, approval, publication, implementation, and maintenance.
D. feasibility, development, approval, implementation, and integration.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
The common steps used the the development of security policy are initiation of the project, evaluation, development, approval, publication, implementation, and maintenance. The other choices listed are the phases of the software development life cycle and not the step used to develop ducuments such as Policies, Standards, etc...
Reference: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.

NEW QUESTION: 83
A variation of the application layer firewall is called a:
A. Current Level Firewall.
B. Cache Level Firewall.
C. Session Level Firewall.
D. Circuit Level Firewall.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Terminology can be confusing between the different souces as both CBK and AIO3 call an application layer firewall a proxy and proxy servers are generally classified as either circuit-level proxies or application level proxies.
The distinction is that a circuit level proxy creates a conduit through which a trusted host can communicate with an untrusted one and doesn't really look at the application contents of the packet (as an application level proxy does). SOCKS is one of the better known circuit-level proxies.
Firewalls
Packet Filtering Firewall - First Generation
n Screening Router
n Operates at Network and Transport level
n Examines Source and Destination IP Address
n Can deny based on ACLs
n Can specify Port
Application Level Firewall - Second Generation
n Proxy Server
n Copies each packet from one network to the other
n Masks the origin of the data
n Operates at layer 7 (Application Layer)
n Reduces Network performance since it has do analyze each packet and decide what to do with it.
n Also Called Application Layer Gateway
Stateful Inspection Firewalls - Third Generation
n Packets Analyzed at all OSI layers
n Queued at the network level
n Faster than Application level Gateway
Dynamic Packet Filtering Firewalls - Fourth Generation
n Allows modification of security rules
n Mostly used for UDP
n Remembers all of the UDP packets that have crossed the network's perimeter, and it decides whether to enable packets to pass through the firewall.
Kernel Proxy - Fifth Generation
n Runs in NT Kernel

n Uses dynamic and custom TCP/IP-based stacks to inspect the network packets and to enforce security policies.
"Current level firewall" is incorrect. This is an amost-right-sounding distractor to confuse the unwary.
"Cache level firewall" is incorrect. This too is a distractor.
"Session level firewall" is incorrect. This too is a distractor.
References
CBK, p. 466 - 467
AIO3, pp. 486 - 490
CISSP Study Notes from Exam Prep Guide

NEW QUESTION: 84
Which of the following is NOT a property of a one-way hash function?
A. It converts a message of a fixed length into a message digest of arbitrary length.
B. It is computationally infeasible to construct two different messages with the same digest.
C. It converts a message of arbitrary length into a message digest of a fixed length.
D. Given a digest value, it is computationally infeasible to find the corresponding message.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
An algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string.
A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.
A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message," and the hash value is sometimes called the message digest or simply digest.
The ideal cryptographic hash function has four main or significant properties:
it is easy (but not necessarily quick) to compute the hash value for any given message it is infeasible to generate a message that has a given hash
it is infeasible to modify a message without changing the hash
it is infeasible to find two different messages with the same hash
Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for functions with rather different properties and purposes.
Source:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

and
http://en.wikipedia.org/wiki/Cryptographic_hash_function

NEW QUESTION: 85
How should a risk be HANDLED when the cost of the countermeasure OUTWEIGHS the cost of the risk?
A. Reject the risk
B. Perform another risk analysis
C. Accept the risk
D. Reduce the risk
Answer: C (LEAVE A REPLY)
Which means the company understands the level of risk it is faced.
The following answers are incorrect because :
Reject the risk is incorrect as it means ignoring the risk which is dangerous.
Perform another risk analysis is also incorrect as the existing risk analysis has already
shown the results.
Reduce the risk is incorrect is applicable after implementing the countermeasures.
Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 39

NEW QUESTION: 86
Which of the following is NOT a task normally performed by a Computer Incident Response Team (CIRT)?
A. Develop an information security policy.
B. Coordinate the distribution of information pertaining to the incident to the appropriate parties.
C. Mitigate risk to the enterprise.
D. Assemble teams to investigate the potential vulnerabilities.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Writing a corporate security policy is normally a task of upper management in an organization. Other tasks would usually be performed by a Computer Incident Response Team.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
64).

NEW QUESTION: 87
Which of the following would be used to implement Mandatory Access Control (MAC)?
A. Clark-Wilson Access Control
B. Role-based access control
C. Lattice-based access control
D. User dictated access control

Answer: C (LEAVE A REPLY)

Explanation/Reference:

The lattice is a mechanism use to implement Mandatory Access Control (MAC) Under Mandatory Access Control (MAC) you have:

Mandatory Access Control

Under Non Discretionary Access Control (NDAC) you have:

Rule-Based Access Control

Role-Based Access Control

Under Discretionary Access Control (DAC) you have:

Discretionary Access Control

The Lattice Based Access Control is a type of access control used to implement other access control method. A lattice is an ordered list of elements that has a least upper bound and a most lower bound. The lattice can be used for MAC, DAC, Integrity level, File Permission, and more For example in the case of MAC, if we look at common government classifications, we have the following:

TOP SECRET

SECRET ----------I am the user at secret

CONFIDENTIAL

SENSITIVE BUT UNCLASSIFIED

UNCLASSIFIED

If you look at the diagram above where I am a user at SECRET it means that I can access document at lower classification but not document at TOP SECRET. The lattice is a list of ORDERED ELEMENT, in this case the ordered elements are classification levels. My least upper bound is SECRET and my most lower bound is UNCLASSIFIED.

However the lattice could also be used for Integrity Levels such as:

VERY HIGH

HIGH

MEDIUM ----------I am a user, process, application at the medium level

LOW

VERY LOW

In the case of of Integrity levels you have to think about TRUST. Of course if I take for example the the VISTA operating system which is based on Biba then Integrity Levels would be used. As a user having access to the system I cannot tell a process running with administrative privilege what to do. Else any users on the system could take control of the system by getting highly privilege process to do things on their behalf. So no read down would be allowed in this case and this is an example of the Biba model.

Last but not least the lattice could be use for file permissions:

RWX

RW ---------User at this level

R

If I am a user with READ and WRITE (RW) access privilege then I cannot execute the file because I do not have execute permission which is the X under linux and UNIX.

Many people confuse the Lattice Model and many books says MAC = LATTICE, however the lattice can be use for other purposes.
There is also Role Based Access Control (RBAC) that exists out there. It COULD be used to simulate MAC but it is not MAC as it does not make use of Label on objects indicating sensitivity and categories. MAC also require a clearance that dominates the object.
You can get more info about RBAC at:http://csrc.nist.gov/groups/SNS/rbac/faq.html#03 Also note that many book uses the same acronym for Role Based Access Control and Rule Based Access Control which is RBAC, this can be confusing.
The proper way of writing the acronym for Rule Based Access Control is RuBAC, unfortunately it is not commonly used.
References:
There is a great article on technet that talks about the lattice in VISTA:
http://blogs.technet.com/b/steriley/archive/2006/07/21/442870.aspx
also see:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).
and
http://www.microsoft-watch.com/content/vista/gaging_vistas_integrity.html

NEW QUESTION: 88
Which of the following devices enables more than one signal to be sent out simultaneously over one physical circuit?
A. Router
B. Multiplexer
C. Channel service unit/Data service unit (CSU/DSU)
D. Wan switch
Answer: B (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Multiplexers are devices that enable enables more than one signal to be sent out simultaneously over one physical circuit.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
118).

NEW QUESTION: 89
During which phase of an IT system life cycle are security requirements developed?
A. Operation
B. Initiation
C. Functional design analysis and Planning

D. Implementation

Answer: (SHOW ANSWER)

Section: Security Operation Adimnistration

Explanation/Reference:

The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems.

The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:

This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:

* Conduct the risk assessment and use the results to supplement the baseline security controls;
* Analyze security requirements;
* Perform functional and security testing;
* Prepare initial documents for system certification and accreditation; and
* Design security architecture.

Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.

Shon Harris' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:

Project initiation

Functional design analysis and planning

System design specifications

Software development

Installation

Maintenance support

Revision and replacement

According to the author (Shon Harris), security requirements should be developed during the functional design analysis and planning phase.

SDLC POSITIONING FROM NIST 800-64

SDLC Positioning in the enterprise

Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and

Enterprise Architecture (EA) processes to establish insight into the agency's vital business operations, their supporting assets, and existing interdependencies and relationships.
With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program's cost- effective performance as well as articulate its business impact and value to the agency.
SDLC OVERVIEW FROM NIST 800-64
SDLC Overview from NIST 800-64 Revision 2
NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of the phases of the SDLC. You will find a copy at: http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf DISCUSSION:
Different sources present slightly different info as far as the phases names are concerned.
People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development Life Cycle has slightly different names, the activities mostly remains the same.
NIST clearly specifies that Security requirements would be considered throughout ALL of the phases. The keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the correct choice.
Within the NIST standard they use different phase, howeverr under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it become easier to come out with the answer to this question. Here is what is stated:
The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.
At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage.
By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.
NIST says:
NIST`s Information Technology Laboratory recently issued Special Publication (SP) 800-64, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.
I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.
References:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956 and NIST S-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf and
http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlc-system-development

NEW QUESTION: 90
Which of the following access control models requires defining classification for objects?
A. Role-based access control
B. Discretionary access control
C. Identity-based access control
D. Mandatory access control
Answer: D (LEAVE A REPLY)
Explanation/Reference:
With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and classification of objects.
The Following answers were incorrect:
Identity-based Access Control is a type of Discretionary Access Control (DAC), they are synonymous.
Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC or RBAC) are types of Non Discretionary Access Control (NDAC).
Tip:
When you have two answers that are synonymous they are not the right choice for sure.
There is only one access control model that makes use of Label, Clearances, and Categories, it is Mandatory Access Control, none of the other one makes use of those items.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION: 91
Valuable paper insurance coverage does not cover damage to which of the following?
A. Inscribed, printed and Written documents
B. Manuscripts
C. Records
D. Money and Securities
Answer: D (LEAVE A REPLY)
Explanation/Reference:
All businesses are driven by records. Even in today's electronic society businesses generate mountains of critical documents everyday. Invoices, client lists, calendars, contracts, files, medical records, and innumerable other records are generated every day.
Stop and ask yourself what happens if your business lost those documents today.

Valuable papers business insurance coverage provides coverage to your business in case of a loss of vital records. Over the years policy language has evolved to include a number of different types of records.

Generally, the policy will cover "written, printed, or otherwise inscribed documents and records, including books, maps, films, drawings, abstracts, deeds, mortgages, and manuscripts." But, read the policy coverage carefully. The policy language typically "does not mean "money" or "securities," converted data,programs or instructions used in your data processing operations, including the materials on which the data is recorded."

The coverage is often included as a part of property insurance or as part of a small business owner policy.

For example, a small business owner policy includes in many cases valuable papers coverage up to $25,000.

It is important to realize what the coverage actually entails and, even more critical, to analyze your business to determine what it would cost to replace records.

The coverage pays for the loss of vital papers and the cost to replace the records up to the limit of the insurance and after application of any deductible. For example, the insurer will pay to have waterlogged papers dried and reproduced (remember, fires are put out by water and the fire department does not stop to remove your book keeping records). The insurer may cover temporary storage or the cost of moving records to avoid a loss.

For some businesses, losing customer lists, some business records, and contracts, can mean the expense and trouble of having to recreate those documents, but is relatively easy and a low level risk and loss.

Larger businesses and especially professionals (lawyers, accountants, doctors) are in an entirely separate category and the cost of replacement of documents is much higher. Consider, in analyzing your business and potential risk, what it would actually cost to reproduce your critical business records. Would you need to hire temporary personnel? How many hours of productivity would go into replacing the records? Would you need to obtain originals? Would original work need to be recreated (for example, home inspectors, surveyors, cartographers)?

Often when a business owner considers the actual cost related to the reproduction of records, the owner quickly realizes that their business insurance policy limits for valuable papers coverage is woefully inadequate.

Insurers (and your insurance professional)will often suggest higher coverages for valuable papers. The extra premium is often worth the cost and should be considered.

Finally, most policies will require records to be protected. You need to review your declarations pages and speak with your insurer to determine what is required. Some insurers may offer discounted coverage if there is a document retention and back up plan in place and followed. There are professional organizations that can assist your business in designing a records management policy to lower the risk (and your premiums). For example, ARMA International has been around since 1955 and its members consist of some of the top document retention and storage companies.

Reference(s) used for this question:

http://businessinsure.about.com/od/propertyinsurance/f/vpcov.htm

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 92
What size is an MD5 message digest (hash)?
A. 128 bits
B. 160 bits
C. 256 bits
D. 128 bytes
Answer: (SHOW ANSWER)
Explanation/Reference:
MD5 is a one-way hash function producing a 128-bit message digest from the input message, through 4 rounds of transformation. MD5 is specified as an Internet Standard (RFC1312).
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 93
How should a doorway of a manned facility with automatic locks be configured?
A. It should be configured to be fail-secure.
B. It should be configured to be fail-safe.
C. It should have a door delay cipher lock.
D. It should not allow piggybacking.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Access controls are meant to protect facilities and computers as well as people.
In some situations, the objectives of physical access controls and the protection of people's lives may come into conflict. In theses situations, a person's life always takes precedence.
Many physical security controls make entry into and out of a facility hard, if not impossible. However, special consideration needs to be taken when this could affect lives. In an information processing facility, different types of locks can be used and piggybacking should be prevented, but the issue here with automatic locks is that they can either be configured as fail-safe or fail-secure.
Since there should only be one access door to an information processing facility, the automatic lock to the only door to a man-operated room must be configured to allow people out in case of emergency, hence to be fail-safe (sometimes called fail-open), meaning that upon fire alarm activation or electric power failure,

the locking device unlocks. This is because the solenoid that maintains power to the lock to keep it in a locked state fails and thus opens or unlocks the electronic lock.
Fail Secure works just the other way. The lock device is in a locked or secure state with no power applied.
Upon authorized entry, a solinoid unlocks the lock temporarily. Thus in a Fail Secure lock, loss of power of fire alarm activation causes the lock to remain in a secure mode.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 451). McGraw-Hill. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20249-20251). Auerbach Publications. Kindle Edition.

NEW QUESTION: 94
What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?
A. Biometrics
B. Micrometrics
C. Macrometrics
D. MicroBiometrics
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

NEW QUESTION: 95
What is the PRIMARY reason to maintain the chain of custody on evidence that has been collected?
A. To ensure that no evidence is lost.
B. To ensure that all possible evidence is gathered.
C. To ensure that it will be admissible in court
D. To ensure that incidents were handled with due care and due diligence.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
This is the PRIMARY reason for the chain of custody of evidence. Evidence must be controlled every step of the way. If it is not, the evidence can be tampered with and ruled inadmissable. The Chain of Custody will include a detailed record of:
Who obtained the evidence
What was the evidence
Where and when the evidence was obtained

Who secured the evidence
Who had control or possession of the evidence
The following answers are incorrect because :
To ensure that no evidence is lost is incorrect as it is not the PRIMARY reason.
To ensure that all possible evidence is gathered is also incorrect as it is not the PRIMARY reason.
To ensure that incidents were handled with due care and due diligence is also incorrect as it is also not the PRIMARY reason.
The chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to establish that it is sufficiently trustworthy to be presented as evidence in court.
Because electronic evidence can be easily modified, a clearly defined chain of custody demonstrates that the evidence is trustworthy which would make it admissible in court.
Reference : Shon Harris AIO v3 , Chapter-10: Law, Investigation, and Ethics , Page : 727

NEW QUESTION: 96
What is the goal of the Maintenance phase in a common development process of a security policy?
A. to review the document on the specified review date
B. publication within the organization
C. to write a proposal to management that states the objectives of the policy
D. to present the document to an approving body
Answer: (SHOW ANSWER)
Explanation/Reference:
"publication within the organization" is the goal of the Publication Phase "write a proposal to management that states the objectives of the policy" is part of Initial and Evaluation Phase "Present the document to an approving body" is part of Approval Phase.
Reference: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 3, 2002, Auerbach Publications.
Also: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 286).

NEW QUESTION: 97
Which of the following is NOT a property of the Rijndael block cipher algorithm?
A. The key sizes must be a multiple of 32 bits
B. Maximum block size is 256 bits
C. Maximum key size is 512 bits
D. The key size does not have to match the block size
Answer: C (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
The above statement is NOT true and thus the correct answer. The maximum key size on Rijndael is 256 bits.

There are some differences between Rijndael and the official FIPS-197 specification for AES.
Rijndael specification per se is specified with block and key sizes that must be a multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits. Namely, Rijndael allows for both key and block sizes to be chosen independently from the set of { 128, 160, 192, 224, 256 } bits. (And the key size does not in fact have to match the block size).
However, FIPS-197 specifies that the block size must always be 128 bits in AES, and that the key size may be either 128, 192, or 256 bits. Therefore AES-128, AES-192, and AES-256 are actually:
Key Size (bits) Block Size (bits)
AES-128 128 128
AES-192 192 128
AES-256 256 128
So in short:
Rijndael and AES differ only in the range of supported values for the block length and cipher key length.
For Rijndael, the block length and the key length can be independently specified to any multiple of 32 bits, with a minimum of 128 bits, and a maximum of 256 bits.
AES fixes the block length to 128 bits, and supports key lengths of 128, 192 or 256 bits only.
References used for this question:
http://blogs.msdn.com/b/shawnfa/archive/2006/10/09/the-differences-between-rijndael-and-aes.aspx and
http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf

NEW QUESTION: 98
Crackers today are MOST often motivated by their desire to:
A. Help the community in securing their networks.
B. Seeing how far their skills will take them.
C. Getting recognition for their actions.
D. Gaining Money or Financial Gains.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
A few years ago the best choice for this question would have been seeing how far their skills can take them. Today this has changed greatly, most crimes committed are financially motivated.
Profit is the most widespread motive behind all cybercrimes and, indeed, most crimes- everyone wants to make money. Hacking for money or for free services includes a smorgasbord of crimes such as embezzlement, corporate espionage and being a "hacker for hire". Scams are easier to undertake but the likelihood of success is much lower. Money-seekers come from any lifestyle but those with persuasive skills make better con artists in the same way as those who are exceptionally tech-savvy make better "hacks for hire".
"White hats" are the security specialists (as opposed to Black Hats) interested in helping the community in securing their networks. They will test systems and network with the owner authorization.
A Black Hat is someone who uses his skills for offensive purpose. They do not seek authorization before they attempt to comprise the security mechanisms in place.

"Grey Hats" are people who sometimes work as a White hat and other times they will work as a "Black Hat", they have not made up their mind yet as to which side they prefer to be.
The following are incorrect answers:
All the other choices could be possible reasons but the best one today is really for financial gains.
References used for this question:
http://library.thinkquest.org/04oct/00460/crimeMotives.html
and
http://www.informit.com/articles/article.aspx?p=1160835
and
http://www.aic.gov.au/documents/1/B/A/%7B1BA0F612-613A-494D-B6C5-06938FE8BB53%7Dhtcb006.pdf

NEW QUESTION: 99
In which layer of the OSI Model are connection-oriented protocols located in the TCP/IP suite of protocols?
A. Transport layer
B. Application layer
C. Physical layer
D. Network layer
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Connection-oriented protocols such as TCP provides reliability.
It is the responsibility of such protocols in the transport layer to ensure every byte is accounted for. The network layer does not provide reliability. It only privides the best route to get the traffic to the final destination address.
For your exam you should know the information below about OSI model:
The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.
The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.
OSI Model
Image source: http://www.petri.co.il/images/osi_model.JPG
PHYSICAL LAYER
The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical,

and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts

How the receiving station delimits a frame

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.

Frame sequencing: transmits/receives frames sequentially.

Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame delimiting: creates and recognizes frame boundaries.

Frame error checking: checks received frames for integrity.

Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: routes frames among networks.

Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.

Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.

Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.

Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

The session layer allows session establishment between processes running on different stations. It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.
The presentation layer provides:
Character code translation: for example, ASCII to EBCDIC.
Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
Data compression: reduces the number of bits that need to be transmitted on the network.
Data encryption: encrypt data for security purposes. For example, password encryption.
APPLICATION LAYER
The application layer serves as the window for users and application processes to access network services.
This layer contains a variety of commonly needed functions:
Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals
The following were incorrect answers:
Application Layer - The application layer serves as the window for users and application processes to access network services.
Network layer - The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.
Physical Layer - The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 260
and
Official ISC2 guide to CISSP CBK 3rd Edition Page number 287
and
http://en.wikipedia.org/wiki/Tcp_protocol

NEW QUESTION: 100
What is the 802.11 standard related to?
A. Public Key Infrastructure (PKI)
B. Wireless network communications

C. Packet-switching technology
D. The OSI/ISO model
Answer: B (LEAVE A REPLY)
Explanation/Reference:
The 802.11 standard outlines how wireless clients and APs communicate, lays out the specifications of their interfaces, dictates how signal transmission should take place, and describes how authentication, association, and security should be implemeted.
The following answers are incorrect:
Public Key Infrastructure (PKI) Public Key Infrastructure is a supporting infrastructure to manage public keys. It is not part of the IEEE 802 Working Group standard.
Packet-switching technology A packet-switching technology is not included in the IEEE 802 Working Group standard. It is a technology where-in messages are broken up into packets, which then travel along different routes to the destination.
The OSI/ISO model The Open System Interconnect model is a sevel-layer model defined as an international standard describing network communications.
The following reference(s) were/was used to create this question:
Source: Shon Harris - "All-in-One CISSP Exam Guide" Fourth Edition; Chapter 7 - Telecommunications and Network Security: pg. 624.
802.11 refers to a family of specifications developed by the IEEE for Wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997. There are several specifications in the 802.11 family:
802.11 # applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
802.11a # an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
802.11b (also referred to as 802.11 High Rate or Wi-Fi) # an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
802.11g # applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.
Source: 802.11 Planet's web site.

NEW QUESTION: 101
A channel within a computer system or network that is designed for the authorized transfer of information is identified as a(n)?
A. Covert channel
B. Overt channel
C. Opened channel
D. Closed channel

Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
An overt channel is a path within a computer system or network that is designed for the authorized transfer of data. The opposite would be a covert channel which is an unauthorized path.
A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way. Receiving information in this manner clearly violates the system's security policy.
All of the other choices are bogus detractors.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 219.
and
Shon Harris, CISSP All In One (AIO), 6th Edition , page 380
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 378). McGraw-Hill. Kindle Edition.

NEW QUESTION: 102
The typical computer fraudsters are usually persons with which of the following characteristics?
A. They have had previous contact with law enforcement
B. They conspire with others
C. They hold a position of trust
D. They deviate from the accepted norms of society
Answer: C (LEAVE A REPLY)
These people, as employees, are trusted to perform their duties honestly and not take advantage of the trust placed in them.
The following answers are incorrect:
They have had previous contact with law enforcement. Is incorrect because most often it is a person that holds a position of trust and this answer implies they have a criminal background. This type of individual is typically not in a position of trust within an organization.
They conspire with others. Is incorrect because they typically work alone, often as a form of retribution over a percieved injustice done to them.
They deviate from the accepted norms of society. Is incorrect because while the nature of fraudsters deviate from the norm, the fraudsters often hold a position of trust within the organization.

NEW QUESTION: 103
What is the primary role of smartcards in a PKI?
A. Transparent renewal of user keys

B. Easy distribution of the certificates between the users
C. Fast hardware encryption of the raw data
D. Tamper resistant, mobile storage and application of private keys of the users
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page
139;
SNYDER, J., What is a SMART CARD?.
Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance Security Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures.
Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip.
It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including:
physical attack of various forms (microprobing, drills, files, solvents, etc.) freezing the device applying out-of-spec voltages or power surges applying unusual clock signals inducing software errors using radiation measuring the precise time and power requirements of certain operations (see power analysis) Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of-specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled.
Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

NEW QUESTION: 104
Which of the following is NOT an administrative control?
A. Logical access control mechanisms
B. Screening of personnel
C. Development of policies, standards, procedures and guidelines
D. Change control procedures

Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
It is considered to be a technical control.
Logical is synonymous with Technical Control. That was the easy answer.
There are three broad categories of access control: Administrative, Technical, and Physical.
Each category has different access control mechanisms that can be carried out manually or automatically. All of these access control mechanisms should work in concert with each other to protect an infrastructure and its data.
Each category of access control has several components that fall within it, as shown here:
Administrative Controls
* Policy and procedures
* Personnel controls
* Supervisory structure
* Security-awareness training
* Testing
Physical Controls
Network segregation
Perimeter security
Computer controls
Work area separation
Data backups
Technical Controls
System access
Network architecture
Network access
Encryption and protocols
Control zone
Auditing
The following answers are incorrect :
Screening of personnel is considered to be an administrative control
Development of policies, standards, procedures and guidelines is considered to be an administrative control Change control procedures is considered to be an administrative control.
Reference : Shon Harris AIO v3 , Chapter - 3 : Security Management Practices , Page : 52-54

NEW QUESTION: 105
Which of the following are WELL KNOWN PORTS assigned by the IANA?
A. Ports 0 to 255
B. Ports 0 to 1024
C. Ports 0 to 1023
D. Ports 0 to 127

Answer: C (LEAVE A REPLY)
Explanation/Reference:
The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports. The range for assigned "Well Known" ports managed by the IANA (Internet Assigned Numbers Authority) is 0-1023.
Source: iana.org: port assignments.

NEW QUESTION: 106
Which of the following access methods is used by Ethernet?
A. CSMA/CD.
B. CSU/DSU.
C. TCP/IP.
D. FIFO.
Answer: (SHOW ANSWER)
Explanation/Reference:
Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to minimize the effect of broadcast collisions.
The following answers are incorrect:
CSU/DSU Is incorrect because Channel Service Unit/Digital Service Unit(CSU/DSU) is a digital interface normally used to connect a router to a digital circuit.
TCP/IP Is incorrect because Transmission Control Protocol/Internet Protocol(TCP/IP) is a network protocol not an access method.
FIFO Is incorrect as it is a distractor. First In, First Out (FIFO) is typically a processing methodology in which first come, first served.
Ethernet is a frame based network technology.
References:
OIG CBK Telecommunications and Network Security (pages 437 - 438)
Wikipedia http://en.wikipedia.org/wiki/FIFO

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 107
What is called the percentage of valid subjects that are falsely rejected by a Biometric Authentication system?

A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. True Rejection Rate (TRR) or Type III Error
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation
Explanation/Reference:
The percentage of valid subjects that are falsely rejected is called the False Rejection Rate (FRR) or Type I Error.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

NEW QUESTION: 108
What can be best defined as the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment?
A. Risk management
B. Risk analysis
C. Threat analysis
D. Due diligence
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Threat analysis is the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
The following answers are incorrect:
Risk analysis is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.
Risk analysis is synonymous with risk assessment and part of risk management, which is the ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost- effective controls to achieve and maintain an acceptable level or risk.
Due Diligence is identifying possible risks that could affect a company based on best practices and standards.
Reference(s) used for this question:
STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page B-3).

NEW QUESTION: 109

What is the highest amount a company should spend annually on countermeasures for protecting an asset valued at $1,000,000 from a threat that has an annualized rate of occurrence (ARO) of once every five years and an exposure factor (EF) of 30%?

A. $300,000

B. $150,000

C. $60,000

D. $1,500

Answer: C (LEAVE A REPLY)

Section: Risk, Response and Recovery

Explanation/Reference:

The cost of a countermeasure should not be greater in cost than the risk it mitigates (ALE). For a quantitative risk assessment, the equation is ALE = ARO x SLE where the SLE is calculated as the product of asset value x exposure factor. An event that happen once every five years would have an ARO of .2 (1 divided by 5).

SLE = Asset Value (AV) x Exposure Fact (EF)

SLE = 1,000,000 x .30 = 300,000

ALE = SLE x Annualized Rate of Occurance (ARO)

ALE = 300,000 x .2 = 60,000

Know your acronyms:

ALE -- Annual loss expectancy

ARO -- Annual rate of occurrence

SLE -- Single loss expectancy

The following are incorrect answers:

$300,000 is incorrect. See the explanation of the correct answer for the correct calculation.

$150,000 is incorrect. See the explanation of the correct answer for the correct calculation.

$1,500 is incorrect. See the explanation of the correct answer for the correct calculation.

Reference(s) used for this question:

Mc Graw Hill, Shon Harris, CISSP All In One (AIO) book, Sixth Edition , Pages 87-88 and Official ISC2 Guide to the CISSP Exam, (OIG), Pages 60-61

NEW QUESTION: 110

A _____ is an information path that is not normally used for communication within a computer system. It is not protected by the any of the systems security mechanisms.

A. Trojaned program

B. Backdoor

C. Covert channel

D. Hijacked session

E. Back-path

Answer: (SHOW ANSWER)

Covert channels can be used as a secret way to convey information to another person or program or for other illicit means.

NEW QUESTION: 111
Which security model introduces access to objects only through programs?
A. The Biba model
B. The Bell-LaPadula model
C. The Clark-Wilson model
D. The information flow model
Answer: C (LEAVE A REPLY)
Explanation/Reference:
In the Clark-Wilson model, the subject no longer has direct access to objects but instead must access them through programs (well -formed transactions).
The Clark-Wilson integrity model provides a foundation for specifying and analyzing an integrity policy for a computing system.
The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules.
Clark-Wilson is more clearly applicable to business and industry processes in which the integrity of the information content is paramount at any level of classification.
Integrity goals of Clark-Wilson model:
Prevent unauthorized users from making modification (Only this one is addressed by the Biba model).
Separation of duties prevents authorized users from making improper modifications.
Well formed transactions: maintain internal and external consistency i.e. it is a series of operations that are carried out to transfer the data from one consistent state to the other.
The following are incorrect answers:
The Biba model is incorrect. The Biba model is concerned with integrity and controls access to objects based on a comparison of the security level of the subject to that of the object.
The Bell-LaPdaula model is incorrect. The Bell-LaPaula model is concerned with confidentiality and controls access to objects based on a comparison of the clearence level of the subject to the classification level of the object.
The information flow model is incorrect. The information flow model uses a lattice where objects are labelled with security classes and information can flow either upward or at the same level. It is similar in framework to the Bell-LaPadula model.
References:
ISC2 Official Study Guide, Pages 325 - 327
AIO3, pp. 284 - 287
AIOv4 Security Architecture and Design (pages 338 - 342)
AIOv5 Security Architecture and Design (pages 341 - 344)
Wikipedia at: https://en.wikipedia.org/wiki/Clark-Wilson_model

NEW QUESTION: 112
What would be the name of a Logical or Virtual Table dynamically generated to restrict the information a user can access in a database?
A. Database Management system
B. Database views
C. Database security
D. Database shadowing
Answer: B (LEAVE A REPLY)
Database views; Database views are mechanisms that restrict
access to the information that a user can access in a database.Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.
Wikipedia has a detailed explantion as well:
In database theory, a view is a virtual or logical table composed of the result set of a query. Unlike ordinary tables (base tables) in a relational database, a view is not part of the physical schema: it is a dynamic, virtual table computed or collated from data in the database. Changing the data in a table alters the data shown in the view.
Views can provide advantages over tables;
They can subset the data contained in a table
They can join and simplify multiple tables into a single virtual table
Views can act as aggregated tables, where aggregated data (sum, average etc.) are calculated and presented as part of the data
Views can hide the complexity of data, for example a view could appear as Sales2000 or Sales2001, transparently partitioning the actual underlying table
Views do not incur any extra storage overhead
Depending on the SQL engine used, views can provide extra security.
Limit the exposure to which a table or tables are exposed to outer world
Just like functions (in programming) provide abstraction, views can be used to create abstraction. Also, just like functions, views can be nested, thus one view can aggregate data from other views. Without the use of views it would be much harder to normalise databases above second normal form. Views can make it easier to create lossless join decomposition.

NEW QUESTION: 113
Computer-generated evidence is considered:
A. Best evidence
B. Second hand evidence
C. Demonstrative evidence
D. Direct evidence
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery

Explanation/Reference:
Computer-generated evidence normally falls under the category of hearsay evidence, or second-hand evidence, because it cannot be proven accurate and reliable. Under the U.S. Federal Rules of Evidence, hearsay evidence is generally not admissible in court. Best evidence is original or primary evidence rather than a copy or duplicate of the evidence. It does not apply to computer-generated evidence. Direct evidence is oral testimony by witness. Demonstrative evidence are used to aid the jury (models, illustrations, charts).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 310).
And: ROTHKE, Ben, CISSP CBK Review presentation on domain 9.

NEW QUESTION: 114
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on :
A. sex of a person
B. physical attributes of a person
C. age of a person
D. voice of a person
Answer: B (LEAVE A REPLY)
Today implementation of fast, accurate reliable and user-acceptable
biometric identification systems is already under way.
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management
Handbook, 4th Edition, Volume 1, Page 7.

NEW QUESTION: 115
Why does fiber optic communication technology have significant security advantage over other transmission technology?
A. Higher data rates can be transmitted.
B. Interception of data traffic is more difficult.
C. Traffic analysis is prevented by multiplexing.
D. Single and double-bit errors are correctable.
Answer: B (LEAVE A REPLY)
It would be correct to select the first answer if the world "security" was not in
the question.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 116
CORRECT TEXT
:A _____ refers to hidden code or instructions added to an application or operating system. This code will not execute until appropriate / predetermined conditions are met.
Answer:

bomb

NEW QUESTION: 117
In the Open Systems Interconnect (OSI) Reference Model, at what level are TCP and UDP provided?
A. Transport
B. Network
C. Presentation
D. Application
Answer: (SHOW ANSWER)
Explanation/Reference:
Transport. The Layer 4 Transport layer supports the TCP and UDP protocols in the OSI Reference Model. This layer creates an end-to-end transportation between peer hosts. The transmission can be connectionless and unreliable such as UDP, or connection-oriented and ensure error-free delivery such as TCP.
The following answers are incorrect:
Network. The Network layer moves information between hosts that are not physically connected. It deals with routing of information. IP is a protocol that is used in Network Layer. TCP and UDP do not reside at the Layer 3 Network Layer in the OSI Reference Model.
Presentation. The Presentation Layer is concerned with the formatting of data into a standard presentation such as
ASCII. TCP and UDP do not reside at the Layer 6 Presentation Layer in the OSI Reference Model.
Application. The Application Layer is a service for applications and Operating Systems data transmission, for example HTTP, FTP and SMTP. TCP and UDP do not reside at the Layer 7 Application Layer in the OSI Reference Model.
The following reference(s) were/was used to create this question:
ISC2 OIG, 2007 p. 411
Shon Harris AIO v.3 p. 424

NEW QUESTION: 118
What kind of encryption is realized in the S/MIME-standard?
A. Asymmetric encryption scheme
B. Password based encryption scheme
C. Public key based, hybrid encryption scheme
D. Elliptic curve based encryption
Answer: (SHOW ANSWER)
S/MIME (for Secure MIME, or Secure Multipurpose Mail Extension) is a security process used for e-mail exchanges that makes it possible to guarantee the confidentiality and non-repudiation of electronic messages. S/MIME is based on the MIME standard, the goal of which is to let users attach files other than ASCII text files to electronic messages. The MIME standard therefore makes it possible to attach all types of files to e-mails.

S/MIME was originally developed by the company RSA Data Security. Ratified in July 1999 by the IETF, S/MIME has become a standard, whose specifications are contained in RFCs 2630 to 2633. How S/MIME works

The S/MIME standard is based on the principle of public-key encryption. S/MIME therefore makes it possible to encrypt the content of messages but does not encrypt the communication.

The various sections of an electronic message, encoded according to the MIME standard, are each encrypted using a session key.

The session key is inserted in each section's header, and is encrypted using the recipient's public key. Only the recipient can open the message's body, using his private key, which guarantees the confidentiality and integrity of the received message.

In addition, the message's signature is encrypted with the sender's private key. Anyone intercepting the communication can read the content of the message's signature, but this ensures the recipient of the sender's identity, since only the sender is capable of encrypting a message (with his private key) that can be decrypted with his public key.

Reference(s) used for this question:

http://en.kioskea.net/contents/139-cryptography-s-mime

RFC 2630: Cryptographic Message Syntax;

OPPLIGER, Rolf, Secure Messaging with PGP and S/MIME, 2000, Artech House;

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 570;

SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

NEW QUESTION: 119

Which protocol is used to send email?

A. File Transfer Protocol (FTP).

B. Post Office Protocol (POP).

C. Network File System (NFS).

D. Simple Mail Transfer Protocol (SMTP).

Answer: D (LEAVE A REPLY)

Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail messages between servers. POP is a protocol used to retrieve e-mail from a mail server. NFS is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture. FTP is the protocol that is used to facilitate file transfer between two machines.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

NEW QUESTION: 120

Which of the following are suitable protocols for securing VPN connections at the lower layers of the OSI model?

A. S/MIME and SSH

B. TLS and SSL
C. IPsec and L2TP
D. PKCS#10 and X.509
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page
467; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

NEW QUESTION: 121
Which of the following is not a preventive login control?
A. Last login message
B. Password aging
C. Minimum password length
D. Account expiration
Answer: A (LEAVE A REPLY)
The last login message displays the last login date and time, allowing a user
to discover if their account was used by someone else. Hence, this is rather a detective
control.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly,
July 1992 (page 63).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 122
Which property ensures that only the intended recipient can access the data and nobody else?
A. Confidentiality
B. Capability
C. Integrity
D. Availability
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:

Confidentiality is defined as the property that ensures that only the intended recipient can access the data and nobody else. It is usually achieve using cryptogrphic methods, tools, and protocols.
Confidentiality supports the principle of "least privilege" by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis. The level of access that an authorized individual should have is at the level necessary for them to do their job. In recent years, much press has been dedicated to the privacy of information and the need to protect it from individuals, who may be able to commit crimes by viewing the information. Identity theft is the act of assuming one's identity through knowledge of confidential information obtained from various sources.
The following are incorrect answers:
Capability is incorrect. Capability is relevant to access control. Capability-based security is a concept in the design of secure computing systems, one of the existing security models. A capability (known in some systems as a key) is a communicable, unforgeable token of authority. It refers to a value that references an object along with an associated set of access rights. A user program on a capability-based operating system must use a capability to access an object. Capability-based security refers to the principle of designing user programs such that they directly share capabilities with each other according to the principle of least privilege, and to the operating system infrastructure necessary to make such transactions efficient and secure.
Integrity is incorrect. Integrity protects information from unauthorized modification or loss.
Availability is incorrect. Availability assures that information and services are available for use by authorized entities according to the service level objective.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 9345-9349). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Capability-based_security

NEW QUESTION: 123
Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered. There are two basic IDS analysis methods that exists. Which of the basic method is more prone to false positive?
A. Pattern Matching (also called signature analysis)
B. Anomaly Detection
C. Host-based intrusion detection
D. Network-based intrusion detection
Answer: (SHOW ANSWER)
Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered.
There are two basic IDS analysis methods:
1.Pattern Matching (also called signature analysis), and
2.Anomaly detection
PATTERN MATCHING Some of the first IDS products used signature analysis as their detection method and simply looked for known characteristics of an attack (such as specific packet sequences or text in the

data stream) to produce an alert if that pattern was detected. If a new or different attack vector is used, it will not match a known signature and, thus, slip past the IDS.

ANOMALY DETECTION Alternately, anomaly detection uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host. Anomalies may include but are not limited to:

Multiple failed log-on attempts Users logging in at strange hours Unexplained changes to system clocks Unusual error messages Unexplained system shutdowns or restarts Attempts to access restricted files

An anomaly-based IDS tends to produce more data because anything outside of the expected behavior is reported. Thus, they tend to report more false positives as expected behavior patterns change. An advantage to anomaly-based IDS is that, because they are based on behavior identification and not specific patterns of traffic, they are often able to detect new attacks that may be overlooked by a signature-based system. Often information from an anomaly-based IDS may be used to create a pattern for a signature-based IDS.

Host Based Intrusion Detection (HIDS) HIDS is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network. This offers unfettered access to system logs, processes, system information, and device information, and virtually eliminates limits associated with encryption. The level of integration represented by HIDS increases the level of visibility and control at the disposal of the HIDS application.

Network Based Intrustion Detection (NIDS) NIDS are usually incorporated into the network in a passive architecture, taking advantage of promiscuous mode access to the network. This means that it has visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network or the systems and applications utilizing the network.

Below you have other ways that instrusion detection can be performed:

Stateful Matching Intrusion Detection Stateful matching takes pattern matching to the next level. It scans for attack signatures in the context of a stream of traffic or overall system behavior rather than the individual packets or discrete system activities. For example, an attacker may use a tool that sends a volley of valid packets to a targeted system. Because all the packets are valid, pattern matching is nearly useless. However, the fact that a large volume of the packets was seen may, itself, represent a known or potential attack pattern. To evade attack, then, the attacker may send the packets from multiple locations with long wait periods between each transmission to either confuse the signature detection system or exhaust its session timing window. If the IDS service is tuned to record and analyze traffic over a long period of time it may detect such an attack. Because stateful matching also uses signatures, it too must be updated regularly and, thus, has some of the same limitations as pattern matching.

Statistical Anomaly-Based Intrusion Detection The statistical anomaly-based IDS analyzes event data by comparing it to typical, known, or predicted traffic profiles in an effort to find potential security breaches. It attempts to identify suspicious behavior by analyzing event data and identifying patterns of entries that deviate from a predicted norm. This type of detection method can be very effective and, at a very high level, begins to take on characteristics seen in IPS by establishing an expected baseline of behavior and acting on divergence from that baseline. However, there are some potential issues that may surface with

a statistical IDS. Tuning the IDS can be challenging and, if not performed regularly, the system will be prone to false positives. Also, the definition of normal traffic can be open to interpretation and does not preclude an attacker from using normal activities to penetrate systems. Additionally, in a large, complex, dynamic corporate environment, it can be difficult, if not impossible, to clearly define "normal" traffic. The value of statistical analysis is that the system has the potential to detect previously unknown attacks. This is a huge departure from the limitation of matching previously known signatures. Therefore, when combined with signature matching technology, the statistical anomaly-based IDS can be very effective.
Protocol Anomaly-Based Intrusion Detection A protocol anomaly-based IDS identifies any unacceptable deviation from expected behavior based on known network protocols. For example, if the IDS is monitoring an HTTP session and the traffic contains attributes that deviate from established HTTP session protocol standards, the IDS may view that as a malicious attempt to manipulate the protocol, penetrate a firewall, or exploit a vulnerability. The value of this method is directly related to the use of well-known or well-defined protocols within an environment. If an organization primarily uses well-known protocols (such as HTTP, FTP, or telnet) this can be an effective method of performing intrusion detection. In the face of custom or nonstandard protocols, however, the system will have more difficulty or be completely unable to determine the proper packet format. Interestingly, this type of method is prone to the same challenges faced by signature-based IDSs. For example, specific protocol analysis modules may have to be added or customized to deal with unique or new protocols or unusual use of standard protocols. Nevertheless, having an IDS that is intimately aware of valid protocol use can be very powerful when an organization employs standard implementations of common protocols.
Traffic Anomaly-Based Intrusion Detection A traffic anomaly-based IDS identifies any unacceptable deviation from expected behavior based on actual traffic structure. When a session is established between systems, there is typically an expected pattern and behavior to the traffic transmitted in that session. That traffic can be compared to expected traffic conduct based on the understandings of traditional system interaction for that type of connection. Like the other types of anomaly-based IDS, traffic anomaly-based IDS relies on the ability to establish "normal" patterns of traffic and expected modes of behavior in systems, networks, and applications. In a highly dynamic environment it may be difficult, if not impossible, to clearly define these parameters.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3664-3686). Auerbach Publications. Kindle Edition. and Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3711-3734). Auerbach Publications. Kindle Edition. and Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3694-3711). Auerbach Publications. Kindle Edition.

NEW QUESTION: 124
Which backup method usually resets the archive bit on the files after they have been backed up?
A. Incremental backup method.
B. Differential backup method.
C. Partial backup method.

D. Tape backup method.

Answer: (SHOW ANSWER)

Section: Risk, Response and Recovery

Explanation/Reference:

The incremental backup method usually resets the archive bit on the files after they have been backed up.

An Incremental Backup will backup all the files that have changed since the last Full Backup (the first time it is run after a full backup was previously completed) or after an Incremental Backup (for the second backup and subsequent backups) and sets the archive bit to 0. This type of backup take less time during the backup phase but it will take more time to restore.

The other answers are all incorrect choices.

The following backup types also exists:

Full Backup - All data are backed up. The archive bit is cleared, which means that it is set to 0.

Differential Backup - Backup the files that have been modified since the last Full Backup. The archive bit does not change. Take more time while the backup phase is performed and take less time to restore.

Reference(s) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

NEW QUESTION: 125

Which one of the following authentication mechanisms creates a problem for mobile users?

A. Mechanisms based on IP addresses

B. Mechanism with reusable passwords

C. one-time password mechanism.

D. challenge response mechanism.

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Anything based on a fixed IP address would be a problem for mobile users because their location and its associated IP address can change from one time to the next. Many providers will assign a new IP every time the device would be restarted. For example an insurance adjuster using a laptop to file claims online. He goes to a different client each time and the address changes every time he connects to the ISP.

NOTE FROM CLEMENT:

The term MOBILE in this case is synonymous with Road Warriors where a user is contantly traveling and changing location. With smartphone today that may not be an issue but it would be an issue for laptops or WIFI tablets. Within a carrier network the IP will tend to be the same and would change rarely. So this question is more applicable to devices that are not cellular devices but in some cases this issue could affect cellular devices as well.

The following answers are incorrect:

mechanism with reusable password. This is incorrect because reusable password mechanism would not present a problem for mobile users. They are the least secure and change only at specific interval.

one-time password mechanism. This is incorrect because a one-time password mechanism would not present a problem for mobile users. Many are based on a clock and not on the IP address of the user. challenge response mechanism. This is incorrect because challenge response mechanism would not present a problem for mobile users.

NEW QUESTION: 126
A trusted system does NOT involve which of the following?
A. Enforcement of a security policy.
B. Sufficiency and effectiveness of mechanisms to be able to enforce a security policy.
C. Assurance that the security policy can be enforced in an efficient and reliable manner.
D. Independently-verifiable evidence that the security policy-enforcing mechanisms are sufficient and effective.
Answer: C (LEAVE A REPLY)
A trusted system is one that meets its intended security requirements. It involves sufficiency and effectiveness, not necessarily efficiency, in enforcing a security policy. Put succinctly, trusted systems have (1) policy, (2) mechanism, and (3) assurance. Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION: 127
What is malware that can spread itself over open network connections?
A. Worm
B. Rootkit
C. Adware
D. Logic Bomb
Answer: (SHOW ANSWER)
Computer worms are also known as Network Mobile Code, or a virus-like bit of code that can replicate itself over a network, infecting adjacent computers.
A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
A notable example is the SQL Slammer computer worm that spread globally in ten minutes on January 25, 2003. I myself came to work that day as a software tester and found all my SQL servers infected and actively trying to infect other computers on the test network.
A patch had been released a year prior by Microsoft and if systems were not patched and exposed to a 376 byte UDP packet from an infected host then system would become compromised.
Ordinarily, infected computers are not to be trusted and must be rebuilt from scratch but the vulnerability could be mitigated by replacing a single vulnerable dll called sqlsort.dll.
Replacing that with the patched version completely disabled the worm which really illustrates to us the importance of actively patching our systems against such network mobile code.

The following answers are incorrect:
-Rootkit: Sorry, this isn't correct because a rootkit isn't ordinarily classified as network mobile code like a worm is. This isn't to say that a rootkit couldn't be included in a worm, just that a rootkit isn't usually classified like a worm. A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.
-Adware: Incorrect answer. Sorry but adware isn't usually classified as a worm. Adware, or advertising-supported software, is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. The term is sometimes used to refer to software that displays unwanted advertisements.
-Logic Bomb: Logic bombs like adware or rootkits could be spread by worms if they exploit the right service and gain root or admin access on a computer.
The following reference(s) was used to create this question:
The CCCure CompTIA Holistic Security+ Tutorial and CBT and http://en.wikipedia.org/wiki/Rootkit and http://en.wikipedia.org/wiki/Computer_worm and http://en.wikipedia.org/wiki/Adware

NEW QUESTION: 128
What is the main difference between computer abuse and computer crime?
A. Intentions of the perpetrator
B. Amount of damage
C. Method of compromise
D. Abuse = company insider; crime = company outsider
Answer: A (LEAVE A REPLY)

NEW QUESTION: 129
Which of the following would provide the BEST stress testing environment taking under consideration and avoiding possible data exposure and leaks of sensitive data?
A. Test environment using test data.
B. Test environment using sanitized live workloads data.
C. Production environment using test data.
D. Production environment using sanitized live workloads data.
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The best way to properly verify an application or system during a stress test would be to expose it to "live" data that has been sanitized to avoid exposing any sensitive information or Personally Identifiable Data

(PII) while in a testing environment. Fabricated test data may not be as varied, complex or computationally demanding as
"live" data. A production environment should never be used to test a product, as a production environment is one where the application or system is being put to commercial or operational use. It is a best practice to perform testing in a non-production environment.
Stress testing is carried out to ensure a system can cope with production workloads, but as it may be tested to destruction, a test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment. If only test data is used, there is no certainty that the system was adequately stress tested.
Incorrect answers:
Test environment using test data. This is incorrect because live data is typically more useful during stress testing Production environment using test data. This is incorrect because the production environment should not be used for testing.
Production environment using live workloads. This is incorrect because the production environment should not be used for testing.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).
And:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 251.
And:

NEW QUESTION: 130
Which of the following protocols operates at the session layer (layer 5)?
A. RPC
B. IGMP
C. LPD
D. SPX
Answer: (SHOW ANSWER)
Remotre Procedure Call (RPC) is the only of the above choices to operate at the session layer (layer 5). All of the other answers were wrong.
LPD operates at layer 7 SPX operates at layer 4 IGMP operates at layer 3.
Reference:
WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April 2002 (page 1).

NEW QUESTION: 131
What is also known as 10Base5?
A. Thinnet
B. Thicknet

C. ARCnet
D. UTP
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Thicknet is a coaxial cable with segments of up to 500 meters, also known as 10Base5. Thinnet is a coaxial cable with segments of up to 185 meters. Unshielded twisted pair (UTP) has three variations: 10 Mbps (10BaseT), 100 Mbps (100BaseT) or 1 Gbps (1000BaseT). ARCnet is a LAN media access method.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
108).

NEW QUESTION: 132
Which of the following statements pertaining to RADIUS is incorrect:
A. A RADIUS server can act as a proxy server, forwarding client requests to other authentication domains.
B. Most of RADIUS clients have a capability to query secondary RADIUS servers for redundancy.
C. Most RADIUS servers have built-in database connectivity for billing and reporting purposes.
D. Most RADIUS servers can work with DIAMETER servers.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
This is the correct answer because it is FALSE.
Diameter is an AAA protocol, AAA stands for authentication, authorization and accounting protocol for computer networks, and it is a successor to RADIUS.
The name is a pun on the RADIUS protocol, which is the predecessor (a diameter is twice the radius).
The main differences are as follows:
Reliable transport protocols (TCP or SCTP, not UDP)
The IETF is in the process of standardizing TCP Transport for RADIUS
Network or transport layer security (IPsec or TLS)
The IETF is in the process of standardizing Transport Layer Security for RADIUS Transition support for RADIUS, although Diameter is not fully compatible with RADIUS Larger address space for attribute-value pairs (AVPs) and identifiers (32 bits instead of 8 bits) Client-server protocol, with exception of supporting some server-initiated messages as well Both stateful and stateless models can be used
Dynamic discovery of peers (using DNS SRV and NAPTR)
Capability negotiation
Supports application layer acknowledgements, defines failover methods and state machines (RFC 3539)
Error notification
Better roaming support
More easily extended; new commands and attributes can be defined

Aligned on 32-bit boundaries
Basic support for user-sessions and accounting
A Diameter Application is not a software application, but a protocol based on the Diameter base protocol (defined in RFC 3588). Each application is defined by an application identifier and can add new command codes and/or new mandatory AVPs. Adding a new optional AVP does not require a new application.
Examples of Diameter applications:
Diameter Mobile IPv4 Application (MobileIP, RFC 4004)
Diameter Network Access Server Application (NASREQ, RFC 4005)
Diameter Extensible Authentication Protocol (EAP) Application (RFC 4072) Diameter Credit-Control Application (DCCA, RFC 4006)
Diameter Session Initiation Protocol Application (RFC 4740)
Various applications in the 3GPP IP Multimedia Subsystem
All of the other choices presented are true. So Diameter is backwork compatible with Radius (to some extent) but the opposite is false.
Reference(s) used for this question:
TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 38.
and
https://secure.wikimedia.org/wikipedia/en/wiki/Diameter_%28protocol%29

NEW QUESTION: 133
DES, 3DES, Blowfish, and AES are all examples of what type of cryptography?
A. Hash Algorithm
B. Secret Key
C. Public Key B. Message Digest
Answer: B (LEAVE A REPLY)

NEW QUESTION: 134
Which of the following phases of a system development life-cycle is most concerned with establishing a good security policy as the foundation for design?
A. Development/acquisition
B. Implementation
C. Initiation
D. Maintenance
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
A security policy is an important document to develop while designing an information system. The security policy begins with the organization's basic commitment to information security formulated as a general policy statement.

The policy is then applied to all aspects of the system design or security solution. The policy identifies security goals (e.g., confidentiality, integrity, availability, accountability, and assurance) the system should support, and these goals guide the procedures, standards and controls used in the IT security architecture design.
The policy also should require definition of critical assets, the perceived threat, and security-related roles and responsibilities.
Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 6).

NEW QUESTION: 135
Which of the following is best provided by symmetric cryptography?
A. Confidentiality
B. Integrity
C. Availability
D. Non-repudiation
Answer: A (LEAVE A REPLY)
Explanation/Reference:
When using symmetric cryptography, both parties will be using the same key for encryption and decryption. Symmetric cryptography is generally fast and can be hard to break, but it offers limited overall security in the fact that it can only provide confidentiality.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 2).

NEW QUESTION: 136
Which of the following would be true about Static password tokens?
A. The owner identity is authenticated by the token
B. The owner will never be authenticated by the token.
C. The owner will authenticate himself to the system.
D. The token does not authenticates the token owner but the system.
Answer: A (LEAVE A REPLY)
Password Tokens Tokens are electronic devices or cards that supply a user's password for them. A token system can be used to supply either a static or a dynamic password. There is a big difference between the static and dynamic systems, a static system will normally log a user in but a dynamic system the user will often have to log themselves in.
Static Password Tokens: The owner identity is authenticated by the token. This is done by the person who issues the token to the owner (normally the employer). The owner of the token is now authenticated by "something you have". The token authenticates the identity of the owner to the information system. An example of this occurring is when an employee swipes his or her smart card over an electronic lock to gain access to a store room.
Synchronous Dynamic Password Tokens:
This system is a lot more complex then the static token password. The synchronous

dynamic password tokens generate new passwords at certain time intervals that are synched with the main system. The password is generated on a small device similar to a pager or a calculator that can often be attached to the user's key ring. Each password is only valid for a certain time period, typing in the wrong password in the wrong time period will invalidate the authentication. The time factor can also be the systems downfall. If a clock on the system or the password token device becomes out of synch, a user can have troubles authenticating themselves to the system.
Asynchronous Dynamic Password Tokens:
The clock synching problem is eliminated with asynchronous dynamic password tokens. This system works on the same principal as the synchronous one but it does not have a time frame. A lot of big companies use this system especially for employee's who may work from home on the companies VPN (Virtual private Network).
Challenge Response Tokens:
This is an interesting system. A user will be sent special "challenge" strings at either random or timed intervals. The user inputs this challenge string into their token device and the device will respond by generating a challenge response. The user then types this response into the system and if it is correct they are authenticated.
Reference(s) used for this question:
http://www.informit.com/guides/content.aspx?g=security&seqNum=146
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 137
What security principle is based on the division of job responsibilities - designed to prevent fraud?
A. Concept of Least Privilege
B. Information Systems Auditing
C. Separation of Duties
D. Mandatory Access Control
Answer: (SHOW ANSWER)

NEW QUESTION: 138

Which of the following proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?

A. Direct evidence.

B. Circumstantial evidence.

C. Conclusive evidence.

D. Corroborative evidence.

Answer: A (LEAVE A REPLY)

Section: Risk, Response and Recovery

Explanation/Reference:

Direct evidence can prove a fact all by itself and does not need backup information to refer to. When using direct evidence, presumptions are not required. One example of direct evidence is the testimony of a witness who saw a crime take place. Although this oral evidence would be secondary in nature, meaning a case could not rest on just it alone, it is also direct evidence, meaning the lawyer does not necessarily need to provide other evidence to back it up. Direct evidence often is based on information gathered from a witness's five senses.

The following answers are incorrect:

Circumstantial evidence. Is incorrect because Circumstantial evidence can prove an intermediate fact that can then be used to deduce or assume the existence of another fact.

Conclusive evidence. Is incorrect because Conclusive evidence is irrefutable and cannot be contradicted. Conclusive evidence is very strong all by itself and does not require corroboration.

Corroborative evidence. Is incorrect because Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand on its own, but is used as a supplementary tool to help prove a primary piece of evidence.

NEW QUESTION: 139

A prolonged high voltage is a:

A. spike

B. blackout

C. surge

D. fault

Answer: (SHOW ANSWER)

Explanation/Reference:

A prolonged high voltage is a surge.

From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

NEW QUESTION: 140

What is called an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets?

A. SYN Flood attack

B. Smurf attack

C. Ping of Death attack
D. Denial of Service (DOS) attack
Answer: (SHOW ANSWER)
Explanation/Reference:
Although it may cause a denial of service to the victim's system, this type of attack is a Smurf attack. A SYN Flood attack uses up all of a system's resources by setting up a number of bogus communication sockets on the victim's system. A Ping of Death attack is done by sending IP packets that exceed the maximum legal length (65535 octets).
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter
11: Application and System Development (page 789).

NEW QUESTION: 141
What layer of the ISO/OSI model do routers normally operate at?
A. Data link layer
B. Session layer
C. Transport layer
D. Network layer
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Routers are switching devices that operate at the network layer (layer 3) by examining network addresses.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
111).

NEW QUESTION: 142
Which of the following reviews system and event logs to detect attacks on the host and determine if the attack was successful?
A. host-based IDS
B. firewall-based IDS
C. bastion-based IDS
D. server-based IDS
Answer: A (LEAVE A REPLY)
Explanation/Reference:
A host-based IDS can review the system and event logs in order to detect an attack on the host and to determine if the attack was successful.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

NEW QUESTION: 143
Who is responsible for initiating corrective measures and capabilities used when there are security violations?
A. Information systems auditor
B. Security administrator
C. Management
D. Data owners
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
Management is responsible for protecting all assets that are directly or indirectly under their control. They must ensure that employees understand their obligations to protect the company's assets, and implement security in accordance with the company policy. Finally, management is responsible for initiating corrective actions when there are security violations.
Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

NEW QUESTION: 144
The Diffie-Hellman algorithm is primarily used to provide which of the following?
A. Confidentiality
B. Key Agreement
C. Integrity
D. Non-repudiation
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
Diffie and Hellman describe a means for two parties to agree upon a shared secret in such a way that the secret will be unavailable to eavesdroppers. This secret may then be converted into cryptographic keying material for other (symmetric) algorithms. A large number of minor variants of this process exist. See RFC
2631 Diffie-Hellman Key Agreement Method for more details.
In 1976, Diffie and Hellman were the first to introduce the notion of public key cryptography, requiring a system allowing the exchange of secret keys over non-secure channels. The Diffie-Hellman algorithm is used for key exchange between two parties communicating with each other, it cannot be used for encrypting and decrypting messages, or digital signature.
Diffie and Hellman sought to address the issue of having to exchange keys via courier and other unsecure means. Their efforts were the FIRST asymmetric key agreement algorithm. Since the Diffie-Hellman algorithm cannot be used for encrypting and decrypting it cannot provide confidentiality nor integrity. This algorithm also does not provide for digital signature functionality and thus non-repudiation is not a choice.
NOTE: The DH algorithm is susceptible to man-in-the-middle attacks.
KEY AGREEMENT VERSUS KEY EXCHANGE

A key exchange can be done multiple way. It can be done in person, I can generate a key and then encrypt the key to get it securely to you by encrypting it with your public key. A Key Agreement protocol is done over a public medium such as the internet using a mathematical formula to come out with a common value on both sides of the communication link, without the ennemy being able to know what the common agreement is.
The following answers were incorrect:
All of the other choices were not correct choices
Reference(s) used for this question:
Shon Harris, CISSP All In One (AIO), 6th edition . Chapter 7, Cryptography, Page 812.
http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
http://www.google.com/patents?vid=4200770

NEW QUESTION: 145
Which of the following is not a DES mode of operation?
A. Cipher block chaining
B. Electronic code book
C. Input feedback
D. Cipher feedback
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation
Explanation/Reference:
Output feedback (OFB) is a DES mode of operation, not input feedback.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 149).

NEW QUESTION: 146
Crackers today are MOST often motivated by their desire to:
A. Help the community in securing their networks.
B. Seeing how far their skills will take them.
C. Getting recognition for their actions.
D. Gaining Money or Financial Gains.
Answer: (SHOW ANSWER)
Section: Malicious Code
Explanation/Reference:
A few years ago the best choice for this question would have been seeing how far their skills can take them.
Today this has changed greatly, most crimes committed are financially motivated.
Profit is the most widespread motive behind all cybercrimes and, indeed, most crimes- everyone wants to make money. Hacking for money or for free services includes a smorgasbord of crimes such as embezzlement, corporate espionage and being a "hacker for hire". Scams are easier to undertake but the

likelihood of success is much lower. Money-seekers come from any lifestyle but those with persuasive skills make better con artists in the same way as those who are exceptionally tech-savvy make better "hacks for hire".
"White hats" are the security specialists (as opposed to Black Hats) interested in helping the community in securing their networks. They will test systems and network with the owner authorization.
A Black Hat is someone who uses his skills for offensive purpose. They do not seek authorization before they attempt to comprise the security mechanisms in place.
"Grey Hats" are people who sometimes work as a White hat and other times they will work as a "Black Hat", they have not made up their mind yet as to which side they prefer to be.
The following are incorrect answers:
All the other choices could be possible reasons but the best one today is really for financial gains.
References used for this question:
http://library.thinkquest.org/04oct/00460/crimeMotives.html
and
http://www.informit.com/articles/article.aspx?p=1160835
and
http://www.aic.gov.au/documents/1/B/A/%7B1BA0F612-613A-494D-B6C5-06938FE8BB53%7Dhtcb006.pdf

NEW QUESTION: 147
Which OSI/ISO layer is responsible for determining the best route for data to be transferred?
A. Session layer
B. Physical layer
C. Network layer
D. Transport layer
Answer: C (LEAVE A REPLY)
The main responsibility of the network layer is to insert information into the packet's header so that it can be properly routed. The protocols at the network layer must determine the best path for the packet to take.
The following answers are incorrect:
Session layer. The session layer is responsible for establishing a connection between two applications.
Physical layer. The physical layer if responsible for converting electronic impulses into bits and vice-versa.
Transport layer. The transport layer is responsible for data transmission and error detection.
The following reference(s) were/was used to create this question:
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, v3, chapter 7: Telecommunications and Network Security (page 422-428). ISC2 Official ISC2 Guide to the CBK (OIG) 2007, p. 409-412

NEW QUESTION: 148

Which TCSEC level is labeled Controlled Access Protection?

A. C1

B. C2

C. C3

D. B1

Answer: B (LEAVE A REPLY)

Explanation/Reference:

C2 is labeled Controlled Access Protection.

The TCSEC defines four divisions: D, C, B and A where division A has the highest security.

Each division represents a significant difference in the trust an individual or organization can place on the evaluated system. Additionally divisions C, B and A are broken into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and A1.

Each division and class expands or modifies as indicated the requirements of the immediately prior division or class.

D - Minimal protection

Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division

C - Discretionary protection

C1 - Discretionary Security Protection

Identification and authentication

Separation of users and data

Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis

Required System Documentation and user manuals

C2 - Controlled Access Protection

More finely grained DAC

Individual accountability through login procedures

Audit trails

Object reuse

Resource isolation

B - Mandatory protection

B1 - Labeled Security Protection

Informal statement of the security policy model

Data sensitivity labels

Mandatory Access Control (MAC) over selected subjects and objects

Label exportation capabilities

All discovered flaws must be removed or otherwise mitigated

Design specifications and verification

B2 - Structured Protection

Security policy model clearly defined and formally documented

DAC and MAC enforcement extended to all subjects and objects

Covert storage channels are analyzed for occurrence and bandwidth

Carefully structured into protection-critical and non-protection-critical elements Design and implementation enable more comprehensive testing and review
Authentication mechanisms are strengthened
Trusted facility management is provided with administrator and operator segregation Strict configuration management controls are imposed
B3 - Security Domains
Satisfies reference monitor requirements
Structured to exclude code not essential to security policy enforcement Significant system engineering directed toward minimizing complexity
Security administrator role defined
Audit security-relevant events
Automated imminent intrusion detection, notification, and response
Trusted system recovery procedures
Covert timing channels are analyzed for occurrence and bandwidth
An example of such a system is the XTS-300, a precursor to the XTS-400
A - Verified protection
A1 - Verified Design
Functionally identical to B3
Formal design and verification techniques including a formal top-level specification Formal management and distribution procedures
An example of such a system is Honeywell's Secure Communications Processor SCOMP, a precursor to the XTS-400
Beyond A1
System Architecture demonstrates that the requirements of self-protection and completeness for reference monitors have been implemented in the Trusted Computing Base (TCB).
Security Testing automatically generates test-case from the formal top-level specification or formal lower-level specifications.
Formal Specification and Verification is where the TCB is verified down to the source code level, using formal verification methods where feasible.
Trusted Design Environment is where the TCB is designed in a trusted facility with only trusted (cleared) personnel.
The following are incorrect answers:
C1 is Discretionary security
C3 does not exists, it is only a detractor
B1 is called Labeled Security Protection.
Reference(s) used for this question:
HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.
and
AIOv4 Security Architecture and Design (pages 357 - 361)
AIOv5 Security Architecture and Design (pages 358 - 362)

NEW QUESTION: 149
Integrity = _____
A. Data being kept correct and current
B. Protection of data from unauthorized users
C. Ability to access data when requested
D. All answers are correct
E. Data being delivered from the source to the intended receiver without being altered
Answer: E (LEAVE A REPLY)

NEW QUESTION: 150
Which of the following can be defined as an Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client?
A. IMAP4
B. SMTP
C. MIME
D. PEM
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines the Internet Message Access Protocol, version 4 (IMAP4) as an Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client. IMAP4 has mechanisms for optionally authenticating a client to a server and providing other security services.
MIME is the MultiPurpose Internet Mail Extension. MIME extends the format of Internet mail to allow non-US- ASCII textual messages, non-textual messages, multipart message bodies, and non-US-ASCII information in message headers.
Simple Mail Transfer Protocol (SMTP) is a TCP-based, application-layer, Internet Standard protocol for moving electronic mail messages from one computer to another.
Privacy Enhanced Mail (PEM) is an Internet protocol to provide data confidentiality, data integrity, and data origin authentication for electronic mail.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 151
Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?
A. Wave pattern motion detectors
B. Capacitance detectors
C. Field-powered devices
D. Audio detectors

Answer: (SHOW ANSWER)

Explanation/Reference:

Capacitance detectors monitor an electrical field surrounding the object being monitored. They are used for spot protection within a few inches of the object, rather than for overall room security monitoring used by wave detectors. Penetration of this field changes the electrical capacitance of the field enough to generate and alarm. Wave pattern motion detectors generate a frequency wave pattern and send an alarm if the pattern is disturbed as it is reflected back to its receiver. Field-powered devices are a type of personnel access control devices. Audio detectors simply monitor a room for any abnormal sound wave generation and trigger an alarm.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 344).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 152

In the context of access control, locks, gates, guards are examples of which of the following?

A. Administrative controls

B. Technical controls

C. Physical controls

D. Logical controls

Answer: C (LEAVE A REPLY)

Administrative, technical and physical controls are categories of access control mechanisms.

Logical and Technical controls are synonymous. So both of them could be eliminated as possible choices.

Physical Controls: These are controls to protect the organization's people and physical environment, such as locks, gates, and guards. Physical controls may be called "operational controls" in some contexts.

Physical security covers a broad spectrum of controls to protect the physical assets (primarily the people) in an organization. Physical Controls are sometimes referred to as "operational" controls in some risk management frameworks. These controls range from doors, locks, and windows to environment controls, construction standards, and guards. Typically, physical security is based on the notion of establishing security zones or concentric areas within a facility that require increased security as you get closer to the valuable assets inside the facility. Security zones are the physical representation of the defense-in-depth principle discussed earlier in this chapter. Typically, security zones are associated with rooms, offices, floors, or smaller elements, such as a cabinet or storage locker. The design of the physical security

controls within the facility must take into account the protection of the asset as well as the individuals working in that area.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1301-1303). Auerbach Publications. Kindle Edition. and Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1312-1318). Auerbach Publications. Kindle Edition.

NEW QUESTION: 153
Which one of the following represents an ALE calculation?
A. single loss expectancy x annualized rate of occurrence.
B. gross loss expectancy x loss frequency.
C. actual replacement cost - proceeds of salvage.
D. asset value x loss expectancy.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Single Loss Expectancy (SLE) is the dollar amount that would be lost if there was a loss of an asset.
Annualized Rate of Occurrence (ARO) is an estimated possibility of a threat to an asset taking place in one year (for example if there is a change of a flood occuring once in 10 years the ARO would be .1, and if there was a chance of a flood occuring once in 100 years then the ARO would be .01).
The following answers are incorrect:
gross loss expectancy x loss frequency. Is incorrect because this is a distractor.
actual replacement cost - proceeds of salvage. Is incorrect because this is a distractor.
asset value x loss expectancy. Is incorrect because this is a distractor.

NEW QUESTION: 154
CORRECT TEXT
The _____ protocol sends passwords in clear text, while _____ encrypts passwords. Both protocols are used by PPP (Point to Point Protocol) to transport IP traffic,
Answer:
CHAP

NEW QUESTION: 155
Which one of the following is used to provide authentication and confidentiality for e-mail messages?
A. Digital signature
B. PGP
C. IPSEC AH
D. MD4
Answer: B (LEAVE A REPLY)
Explanation/Reference:

Instead of using a Certificate Authority, PGP uses a "Web of Trust", where users can certify each other in a mesh model, which is best applied to smaller groups.
In cryptography, a web of trust is a concept used in PGP, GnuPG, and other OpenPGP compatible systems to establish the authenticity of the binding between a public key and its owner. Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such). The web of trust concept was first put forth by PGP creator Phil Zimmermann in 1992 in the manual for PGP version 2.0.
Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, E-mails, files, directories and whole disk partitions to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991.
As per Shon Harris's book:
Pretty Good Privacy (PGP) was designed by Phil Zimmerman as a freeware e-mail security program and was released in 1991. It was the first widespread public key encryption program. PGP is a complete cryptosystem that uses cryptographic protection to protect e-mail and files. It can use RSA public key encryption for key management and use IDEA symmetric cipher for bulk encryption of data, although the user has the option of picking different types of algorithms for these functions. PGP can provide confidentiality by using the IDEA encryption algorithm, integrity by using the MD5 hashing algorithm, authentication by using the public key certificates, and nonrepudiation by using cryptographically signed messages. PGP initially used its own type of digital certificates rather than what is used in PKI, but they both have similar purposes. Today PGP support X.509 V3 digital certificates.
Reference(s) used for this question:
KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 169).
Shon Harris, CISSP All in One book
https://en.wikipedia.org/wiki/Pretty_Good_Privacy
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 156
The "vulnerability of a facility" to damage or attack may be assessed by all of the following except:
A. Inspection
B. History of losses
C. Security controls
D. security budget
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Source: The CISSP Examination Textbook- Volume 2: Practice by S. Rao Vallabhaneni.

NEW QUESTION: 157
In a stateful inspection firewall, data packets are captured by an inspection engine that is operating at the:
A. Network or Transport Layer.

B. Application Layer.
C. Inspection Layer.
D. Data Link Layer.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Most stateful packet inspection firewalls work at the network or transport layers. For the TCP/IP protcol, this allows the firewall to make decisions both on IP addresses, protocols and TCP/UDP port numbers
Application layer is incorrect. This is too high in the OSI stack for this type of firewall.
Inspection layer is incorrect. There is no such layer in the OSI stack.
"Data link layer" is incorrect. This is too low in the OSI stack for this type of firewall.
References:
CBK, p. 466
AIO3, pp. 485 - 486

NEW QUESTION: 158
Which of the following would provide the BEST stress testing environment taking under consideration and avoiding possible data exposure and leaks of sensitive data?
A. Test environment using test data.
B. Test environment using sanitized live workloads data.
C. Production environment using test data.
D. Production environment using sanitized live workloads data.
Answer: (SHOW ANSWER)
Explanation/Reference:
The best way to properly verify an application or system during a stress test would be to expose it to "live" data that has been sanitized to avoid exposing any sensitive information or Personally Identifiable Data (PII) while in a testing environment. Fabricated test data may not be as varied, complex or computationally demanding as "live" data. A production environment should never be used to test a product, as a production environment is one where the application or system is being put to commercial or operational use. It is a best practice to perform testing in a non-production environment.
Stress testing is carried out to ensure a system can cope with production workloads, but as it may be tested to destruction, a test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment. If only test data is used, there is no certainty that the system was adequately stress tested.
Incorrect answers:
Test environment using test data. This is incorrect because live data is typically more useful during stress testing
Production environment using test data. This is incorrect because the production environment should not be used for testing.
Production environment using live workloads. This is incorrect because the production environment should not be used for testing.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).
And:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 251.
And:

NEW QUESTION: 159
Which of the following reviews system and event logs to detect attacks on the host and determine if the attack was successful?
A. host-based IDS
B. firewall-based IDS
C. bastion-based IDS
D. server-based IDS
Answer: A (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:
A host-based IDS can review the system and event logs in order to detect an attack on the host and to determine if the attack was successful.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

NEW QUESTION: 160
Which type of control is concerned with avoiding occurrences of risks?
A. Deterrent controls
B. Detective controls
C. Preventive controls
D. Compensating controls
Answer: (SHOW ANSWER)
Preventive controls are concerned with avoiding occurrences of risks while deterrent controls are concerned with discouraging violations. Detecting controls identify occurrences and compensating controls are alternative controls, used to compensate weaknesses in other controls. Supervision is an example of compensating control. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 161
An access system that grants users only those rights necessary for them to perform their work is operating on which security principle?
A. Discretionary Access
B. Least Privilege

C. Mandatory Access
D. Separation of Duties
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 162
Under the principle of culpable negligence, executives can be held liable for losses that result from computer system breaches if:
A. The company is not a multi-national company.
B. They have not exercised due care protecting computing resources.
C. They have failed to properly insure computer resources against loss.
D. The company does not prosecute the hacker that caused the breach.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Culpable negligence is defined as: Recklessly acting without reasonable caution and putting another person at risk of injury or death (or failing to do something with the same consequences) Where a suspected security breach has been caused (through wilful intent or culpable negligence) disciplinary action may be sought in line with the appropriate misconduct guidelines for internal employees.
By not exercising Due Care and taking the proper actions, the executives would be liable for losses a company has suffered.
Reference(s) used for this question:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
http://www.thefreedictionary.com/culpable+negligence

NEW QUESTION: 163
Which of the following does NOT concern itself with key management?
A. Internet Security Association Key Management Protocol (ISAKMP)
B. Diffie-Hellman (DH)
C. Cryptology (CRYPTO)
D. Key Exchange Algorithm (KEA)
Answer: C (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
Cryptology is the science that includes both cryptography and cryptanalysis and is not directly concerned with key management. Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis.
The following are all concerned with Key Management which makes them the wrong choices:

Internet Security Association Key Management Protocol (ISAKMP) is a key management protocol used by IPSec. ISAKMP (Internet Security Association and Key Management Protocol) is a protocol defined by RFC
2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange. The actual key exchange is done by the Oakley Key Determination Protocol which is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie-Hellman key exchange algorithm.
Diffie-Hellman and one variation of the Diffie-Hellman algorithm called the Key Exchange Algorithm (KEA) are also key exchange protocols. Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. Diffie-Hellman key exchange (D-H) is a specific method of exchanging keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
Reference(s) used for this question:
Mike Meyers CISSP Certification Passport, by Shon Harris and Mike Meyers, page 228.
It is highlighted as an EXAM TIP. Which tells you that it is a must know for the purpose of the exam.
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Chapter 8:
Cryptography (page 713-715).
and
https://en.wikipedia.org/wiki/ISAKMP
and
http://searchsecurity.techtarget.com/definition/cryptology

NEW QUESTION: 164
Communications and network security relates to transmission of which of the following?
A. voice
B. voice and multimedia
C. data and multimedia
D. voice, data and multimedia
Answer: B (LEAVE A REPLY)
From the published (ISC)2 goals for the Certified Information Systems Security Professional candidate: The CISSP candidate should be familiar to communications and network security as it relates to voice, data, multimedia, and facsimile transmissions in terms of local area, wide area, and remote access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 57.

NEW QUESTION: 165

Which of the following is the primary reason why a user would choose a dial-up modem connection to the Internet when they have a faster, secure Internet connection through the organization's network?
A. To access web sites that blocked by the organization's proxy server.
B. To set up public services using the organization's resources.
C. To check their personal e-mail.
D. To circumvent the organization's security policy.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
All the choices above represent examples of circumventing the organization's security policy, which is the primary reason why a user would be using a dial-up Internet connection when a secure connection is available through the organization's network.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1: Understanding Firewalls.

NEW QUESTION: 166
Which of the following statements is true about data encryption as a method of protecting data?
A. It should sometimes be used for password files
B. It is usually easily administered
C. It makes few demands on system resources
D. It requires careful key management
Answer: D (LEAVE A REPLY)
Explanation/Reference:
In cryptography, you always assume the "bad guy" has the encryption algorithm (indeed, many algorithms such as DES, Triple DES, AES, etc. are public domain). What the bad guy lacks is the key used to complete that algorithm and encrypt/decrypt information. Therefore, protection of the key, controlled distribution, scheduled key change, timely destruction, and several other factors require careful consideration. All of these factors are covered under the umbrella term of "key management".
Another significant consideration is the case of "data encryption as a method of protecting data" as the question states. If that data is to be stored over a long period of time (such as on backup), you must ensure that your key management scheme stores old keys for as long as they will be needed to decrypt the information they encrypted.
The other answers are not correct because:
"It should sometimes be used for password files." - Encryption is often used to encrypt passwords stored within password files, but it is not typically effective for the password file itself. On most systems, if a user cannot access the contents of a password file, they cannot authenticate. Encrypting the entire file prevents that access.
"It is usually easily administered." - Developments over the last several years have made cryptography significantly easier to manage and administer. But it remains a significant challenge. This is not a good answer.
"It makes few demands on system resources." - Cryptography is, essentially, a large complex mathematical algorithm. In order to encrypt and decrypt information, the system must perform this

algorithm hundreds, thousands, or even millions/billions/trillions of times. This becomes system resource intensive, making this a very bad answer.
Reference:
Official ISC2 Guide page: 266 (poor explanation)
All in One Third Edition page: 657 (excellent explanation)
Key Management - Page 732, All in One Fourth Edition

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 167
What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?
A. Biometrics
B. Micrometrics
C. Macrometrics
D. MicroBiometrics
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The Answer: Biometrics; Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 37,38.

NEW QUESTION: 168
Which of the following is used to find the Media Access Control address (MAC) that matches with a known Internet Protocol (IP) address?
A. Address Resolution Protocol (ARP).
B. Reverse Address Resolution Protocol (RARP).
C. Internet Control Message protocol (ICMP).
D. User Datagram Protocol (UDP).
Answer: (SHOW ANSWER)
ARP is used to find the Media Access Control address (MAC) that matches with a known Internet Protocol (IP) address.

The Address Resolution Protocol (ARP) is a computer networking protocol for determining a network host's link layer or hardware address when only its Internet Layer (IP) or Network Layer address is known Reverse Address Resolution Protocol (RARP) is used to find the IP address that matches an Ethernet address.
ICMP is a management protocol and messaging service provider for IP (e.g. PING).
UDP runs over IP. It is a best effort protocol that offers no reliability. UDS is used for application such as streaming media, voice over IP, the DNS protocol, as well as the Simple Network Management Protocol (SNMP).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.
also see:
http://en.wikipedia.org/wiki/Address_resolution_protocol

NEW QUESTION: 169
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person. This raised the necessity of answering 2 questions :
A. what was the sex of a person and his age
B. what part of body to be used and how to accomplish identification that is viable
C. what was the age of a person and his income level
D. what was the tone of the voice of a person and his habits
Answer: B (LEAVE A REPLY)
Today implementation of fast, accurate reliable and user-acceptable biometric identification systems is already taking place. Unique physical attributes or behavior of a person are used for that purpose.
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

NEW QUESTION: 170
Which of the following biometric parameters are better suited for authentication use over a long period of time?
A. Iris pattern
B. Voice pattern
C. Signature dynamics
D. Retina pattern
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The iris pattern is considered lifelong. Unique features of the iris are: freckles, rings, rifts, pits, striations, fibers, filaments, furrows, vasculature and coronas. Voice, signature and retina patterns are more likely to change over time, thus are not as suitable for authentication over a long period of time without needing re-enrollment.

Source: FERREL, Robert G, Questions and Answers for the CISSP Exam, domain 1 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

NEW QUESTION: 171
Which of the following is NOT a true statement regarding the implementaton of the 3DES modes?
A. DES-EEE1 uses one key
B. DES-EEE2 uses two keys
C. DES-EEE3 uses three keys
D. DES-EDE2 uses two keys
Answer: A (LEAVE A REPLY)
There is no DES mode call DES-EEE1. It does not exist.
The following are the correct modes for triple-DES (3DES):
DES-EEE3 uses three keys for encryption and the data is encrypted, encrypted, encrypted;
DES-EDE3 uses three keys and encrypts, decrypts and encrypts data.
DES-EEE2 and DES-EDE2 are the same as the previous modes, but the first and third operations use the same key.
Reference(s) used for this question:
Shon Harris, CISSP All In One (AIO) book, 6th edition , page 808
and
Official ISC2 Guide to the CISSP CBK, 2nd Edition (2010) , page 344-345

NEW QUESTION: 172
Which of the following results in the most devastating business interruptions?
A. Loss of Hardware/Software
B. Loss of Data
C. Loss of Communication Links
D. Loss of Applications
Answer: B (LEAVE A REPLY)
Source: Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1.
All of the others can be replaced or repaired. Data that is lost and was not backed up, cannot be restored.

NEW QUESTION: 173
PGP uses which of the following to encrypt data?
A. An asymmetric encryption algorithm
B. A symmetric encryption algorithm
C. A symmetric key distribution system
D. An X.509 digital certificate
Answer: B (LEAVE A REPLY)

Notice that the question specifically asks what PGP uses to encrypt For this, PGP uses an symmetric key algorithm. PGP then uses an asymmetric key algorithm to encrypt the session key and then send it securely to the receiver. It is an hybrid system where both types of ciphers are being used for different purposes.
Whenever a question talks about the bulk of the data to be sent, Symmetric is always best to choice to use because of the inherent speed within Symmetric Ciphers. Asymmetric ciphers are 100 to 1000 times slower than Symmetric Ciphers.
The other answers are not correct because:
"An asymmetric encryption algorithm" is incorrect because PGP uses a symmetric algorithm to encrypt data.
"A symmetric key distribution system" is incorrect because PGP uses an asymmetric algorithm for the distribution of the session keys used for the bulk of the data.
"An X.509 digital certificate" is incorrect because PGP does not use X.509 digital certificates to encrypt the data, it uses a session key to encrypt the data.
References:
Official ISC2 Guide page: 275 All in One Third Edition page: 664 - 665

NEW QUESTION: 174
Which of the following would be LESS likely to prevent an employee from reporting an incident?
A. They are afraid of being pulled into something they don't want to be involved with.
B. The process of reporting incidents is centralized.
C. They are afraid of being accused of something they didn't do.
D. They are unaware of the company's security policies and procedures.
Answer: (SHOW ANSWER)
Section: Analysis and Monitoring
Explanation/Reference:
The reporting process should be centralized else employees won't bother.
The other answers are incorrect because :
They are afraid of being pulled into something they don't want to be involved with is incorrect as most of the employees fear of this and this would prevent them to report an incident.
They are afraid of being accused of something they didn't do is also incorrect as this also prevents them to report an incident.
They are unaware of the company's security policies and procedures is also incorrect as mentioned above.
Reference : Shon Harris AIO v3 , Ch-10 : Laws , Investigatio & Ethics , Page : 675.

NEW QUESTION: 175
Which OSI/ISO layer does a SOCKS server operate at?
A. Session layer
B. Transport layer
C. Network layer

D. Data link layer

Answer: A (LEAVE A REPLY)

Section: Network and Telecommunications

Explanation/Reference:

A SOCKS based server operates at the Session layer of the OSI model.

SOCKS is an Internet protocol that allows client-server applications to transparently use the services of a network firewall. SOCKS is an abbreviation for "SOCKetS". As of Version 5 of SOCK, both UDP and TCP is supported.

One of the best known circuit-level proxies is SOCKS proxy server. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server, without requiring direct "IP-reachability" The protocol was originally developed by David Koblas, a system administrator of MIPS Computer Systems.

After MIPS was taken over by Silicon Graphics in 1992, Koblas presented a paper on SOCKS at that year's Usenix Security Symposium and SOCKS became publicly available. The protocol was extended to version 4 by Ying-Da Lee of NEC.

SOCKS includes two components, the SOCKS server and the SOCKS client.

The SOCKS protocol performs four functions:

Making connection requests

Setting up proxy circuits

Relaying application data

Performing user authentication (optional)

Source:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 96).

and

http://en.wikipedia.org/wiki/SOCKS

and

http://www.faqs.org/rfcs/rfc1928.html

and

The ISC2 OIG on page 619

NEW QUESTION: 176

A contingency plan should address:

A. Potential risks.

B. Residual risks.

C. Identified risks.

D. All answers are correct.

Answer: (SHOW ANSWER)

Explanation/Reference:

Because it is rarely possible or cost effective to eliminate all risks, an attempt is made to reduce risks to an acceptable level through the risk assessment process. This process allows, from a set of potential risks (whether likely or not), to come up with a set of identified, possible risks.
The implementation of security controls allows reducing the identified risks to a smaller set of residual risks. Because these residual risks represent the complete set of situations that could affect system performance, the scope of the contingency plan may be reduced to address only this decreased risk set. As a result, the contingency plan can be narrowly focused, conserving resources while ensuring an effective system recovery capability.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 7).

NEW QUESTION: 177
If your property Insurance has Actual Cash Valuation (ACV) clause, your damaged property will be compensated based on:
A. Value of item on the date of loss
B. Replacement with a new item for the old one regardless of condition of lost item
C. Value of item one month before the loss
D. Value of item on the date of loss plus 10 percent
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
This is called the Actual Cash Value (ACV) or Actual Cost Valuation (ACV) All of the other answers were only detractors. Below you have an explanation of the different types of valuation you could use. It is VERY important for you to validate with your insurer which one applies to you as you could have some very surprising finding the day you have a disaster that takes place.
Replacement Cost
Property replacement cost insurance promises to replace old with new. Generally, replacement of a building must be done on the same premises and used for the same purpose, using materials comparable to the quality of the materials in the damaged or destroyed property.
There are some other limitations to this promise. For example, the cost of repairs or replacement for buildings doesn't include the increased cost associated with building codes or other laws controlling how buildings must be built today. An endorsement adding coverage for the operation of Building Codes and the increased costs associated with complying with them is available separately - usually for additional premium.
In addition, some insurance underwriters will only cover certain property on a depreciated value (actual cash value - ACV) basis even when attached to the building. This includes awnings and floor coverings, appliances for refrigerating, ventilating, cooking, dishwashing, and laundering. Depreciated value also applies to outdoor equipment or furniture.
Actual Cash Value (ACV)

The ACV is the default valuation clause for commercial property insurance. It is also known as depreciated value, but this is not the same as accounting depreciated value. The actual cash value is determined by first calculating the replacement value of the property. The next step involves estimating the amount to be subtracted, which reflects the building's age, wear, and tear.

This amount deducted from the replacement value is known as depreciation. The amount of depreciation is reduced by inflation (increased cost of replacing the property); regular maintenance; and repair (new roofs, new electrical systems, etc.) because these factors reduce the effective age of the buildings.

The amount of depreciation applicable is somewhat subjective and certainly subject to negotiation. In fact, there is often disagreement and a degree of uncertainty over the amount of depreciation applicable to a particular building.

Given this reality, property owners should not leave the determination of depreciation to chance or wait until suffering a property loss to be concerned about it. Every three to five years, property owners should obtain a professional appraisal of the replacement value and depreciated value of the buildings.

The ACV valuation is an option for directors to consider when certain buildings are in need of repair, or budget constraints prevent insuring all of your facilities on a replacement cost basis. There are other valuation options for property owners to consider as well.

Functional Replacement Cost

This valuation method has been available for some time but has not been widely used. It is beginning to show up on property insurance policies imposed by underwriters with concerns about older, buildings. It can also be used for buildings, which are functionally obsolete.

This method provides for the replacement of a building with similar property that performs the same function, using less costly material. The endorsement includes coverage for building codes automatically.

In the event of a loss, the insurance company pays the smallest of four payment options.

1. In the event of a total loss, the insurer could pay the limit of insurance on the building or the cost to replace the building on the same (or different) site with a payment that is "functionally equivalent."
2. In the event of a partial loss, the insurance company could pay the cost to repair or replace the damaged portion in the same architectural style with less costly material (if available).
3. The insurance company could also pay the amount actually spent to demolish the undamaged portion of the building and clear the site if necessary.
4. The fourth payment option is to pay the amount actually spent to repair, or replace the building using less costly materials, if available (Hillman and McCracken 1997).

Unlike the replacement cost valuation method, which excluded certain fixtures and personal property used to service the premises, this endorsement provides functional replacement cost coverage for these items (awnings, floor coverings, appliances, etc.) (Hillman nd McCracken 1997).

As in the standard replacement cost value option, the insured can elect not to repair or replace the property.

Under these circumstances the company pays the smallest of the following:

1. The Limit of Liability
2. The "market value" (not including the value of the land) at the time of the loss. The endorsement defines

"market value" as the price which the property might be expected to realize if ffered for sale in fair market."
3. A modified form of ACV (the amount to repair or replace on he same site with less costly material and in the same architectural tyle, less depreciation) (Hillman and McCracken 1997).
Agreed Value or Agreed Amount
Agreed value or agreed amount is not a valuation method. Instead, his term refers to a waiver of the coinsurance clause in the property insurance policy. Availability of this coverage feature varies among insurers but, it is usually available only when the underwriter has proof (an independent appraisal, or compliance with an insurance company valuation model) of the value of your property.
When do I get paid?
Generally, the insurance company will not pay a replacement cost settlement until the property that was damaged or destroyed is actually repaired or replaced as soon as reasonably possible after the loss. Under no circumstances will the insurance company pay more than your limit of insurance or more than the actual amount you spend to repair or replace the damaged property if this amount is less than the limit of insurance.
Replacement cost insurance terms give the insured the option of settling the loss on an ACV basis. This option may be exercised if you don't plan to replace the building or if you are faced with a significant coinsurance penalty on a replacement cost settlement.
References:
http://www.schirickinsurance.com/resources/value2005.pdf
and
TIPTON, Harold F. & KRAUSE, MICKI
Information Security Management Handbook, 4th Edition, Volume 1
Property Insurance overview, Page 587.

NEW QUESTION: 178
Which of the following is less likely to be used today in creating a Virtual Private Network?
A. L2TP
B. PPTP
C. IPSec
D. L2F
Answer: D (LEAVE A REPLY)
L2F (Layer 2 Forwarding) provides no authentication or encryption. It is a
Protocol that supports the creation of secure virtual private dial-up networks over the
Internet.
At one point L2F was merged with PPTP to produce L2TP to be used on networks and not only on dial up links.
IPSec is now considered the best VPN solution for IP environments.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 507).

NEW QUESTION: 179
Which of the following items is NOT a benefit of cold sites?
A. No resource contention with other organisation
B. Quick Recovery
C. A secondary location is available to reconstruct the environment
D. Low Cost
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
A cold site is a permanent location that provide you with your own space that you can move into in case of a disaster or catastrophe. It is one of the cheapest solution available as a rental place but it is also the one that would take the most time to recover. A cold site usually takes one to two weeks for recoverey.
Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. The plan should include a trategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:
Dedicated site owned or operated by the organization. Also called redundant or alternate sites;
Reciprocal agreement or memorandum of agreement with an internal or external entity; and
Commercially leased facility.
Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types commonly categorized in terms of their operational readiness are cold sites, warm sites, or hot sites. Other variations or combinations of these can be found, but generally all variations retain similar core features found in one of these three site types.
Progressing from basic to advanced, the sites are described below:
Cold Sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.
fWarm Sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.
Hot Sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.
As discussed above, these three alternate site types are the most common. There are also variations, and hybrid mixtures of features from any one of the three. Each organization should evaluate its core requirements in order to establish the most effective solution.
Two examples of variations to the site types are:
fMobile Sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.
fMirrored Sites are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.
There are obvious cost and ready-time differences among the options. In these examples, the mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least

expensive to maintain, although they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours, but the time necessary for equipment installation and setup can increase this response time. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel and/or equipment there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same hazard as the organization's primary site.
The following reference(s) were used for this question:
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

NEW QUESTION: 180
What is the proper term to refer to a single unit of IP data?
A. IP segment.
B. IP datagram.
C. IP frame.
D. IP fragment.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
IP is a datagram based technology.
DIFFERENCE BETWEEN PACKETS AND DATAGRAM
As specified at: http://en.wikipedia.org/wiki/Packet_(information_technology) In general, the term packet applies to any message formatted as a packet, while the term datagram is generally reserved for packets of an "unreliable" service.
A "reliable" service is one that notifies the user if delivery fails, while an "unreliable" one does not notify the user if delivery fails. For example, IP provides an unreliable service.
Together, TCP and IP provide a reliable service, whereas UDP and IP provide an unreliable one. All these protocols use packets, but UDP packets are generally called datagrams.
If a network does not guarantee packet delivery, then it becomes the host's responsibility to provide reliability by detecting and retransmitting lost packets. Subsequent experience on the ARPANET indicated that the network itself could not reliably detect all packet delivery failures, and this pushed responsibility for error detection onto the sending host in any case. This led to the development of the end-to-end principle, which is one of the Internet's fundamental design assumptions.
The following answers are incorrect:
IP segment. Is incorrect because IP segment is a detractor, the correct terminology is TCP segment. IP is a datagram based technology.
IP frame. Is incorrect because IP frame is a detractor, the correct terminology is Ethernet frame. IP is a datagram based technology.
IP fragment. Is incorrect because IP fragment is a detractor.
References:
Wikipedia http://en.wikipedia.org/wiki/Internet_Protocol

NEW QUESTION: 181
One of the following assertions is NOT a characteristic of Internet Protocol Security (IPsec)
A. Data cannot be read by unauthorized parties
B. The identity of all IPsec endpoints are confirmed by other endpoints
C. Data is delivered in the exact order in which it is sent
D. The number of packets being exchanged can be counted.
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
IPSec provide replay protection that ensures data is not delivered multiple times, however IPsec does not ensure that data is delivered in the exact order in which it is sent. IPSEC uses TCP and packets may be delivered out of order to the receiving side depending which route was taken by the packet.
Internet Protocol Security (IPsec) has emerged as the most commonly used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over IP networks. Depending on how IPsec is implemented and configured, it can provide any combination of the following types of protection:
Confidentiality. IPsec can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.
Integrity. IPsec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.
Peer Authentication. Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.
Replay Protection. The same data is not delivered multiple times, and data is not delivered grossly out of order. However, IPsec does not ensure that data is delivered in the exact order in which it is sent.
Traffic Analysis Protection. A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged. However, the number of packets being exchanged can be counted.
Access Control. IPsec endpoints can perform filtering to ensure that only authorized IPsec users can access particular network resources. IPsec endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing.
The following are incorrect answers because they are all features provided by IPSEC:
"Data cannot be read by unauthorized parties" is wrong because IPsec provides confidentiality through the usage of the Encapsulating Security Protocol (ESP), once encrypted the data cannot be read by unauthorized parties because they have access only to the ciphertext. This is accomplished by encrypting data using a cryptographic algorithm and a session key, a value known only to the two parties exchanging data. The data can only be decrypted by someone who has a copy of the session key.

"The identity of all IPsec endpoints are confirmed by other endpoints" is wrong because IPsec provides peer authentication: Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.
"The number of packets being exchanged can be counted" is wrong because although IPsec provides traffic protection where a person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged, the number of packets being exchanged still can be counted.
Reference(s) used for this question:
NIST 800-77 Guide to IPsec VPNs . Pages 2-3 to 2-4

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 182
Which of the following are required for Life-Cycle Assurance?
A. System Architecture and Design specification.
B. Security Testing and Covert Channel Analysis.
C. Security Testing and Trusted distribution.
D. Configuration Management and Trusted Facility Management.
Answer: C (LEAVE A REPLY)
Security testing and trusted distribution are required for Life-Cycle Assurance.
The following answers are incorrect:
System Architecture and Design specification. Is incorrect because System Architecture is not requried for Life-Cycle Assurance.
Security Testing and Covert Channel Analysis. Is incorrect because Covert Channel Analysis is not requried for Life-Cycle Assurance.
Configuration Management and Trusted Facility Management. Is incorrect because Trusted Facility Management. is not requried for Life-Cycle Assurance.

NEW QUESTION: 183
Which of the following access control models requires defining classification for objects?
A. Role-based access control
B. Discretionary access control
C. Identity-based access control
D. Mandatory access control

Answer: D (LEAVE A REPLY)

Section: Access Control

Explanation/Reference:

With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and classification of objects.

The Following answers were incorrect:

Identity-based Access Control is a type of Discretionary Access Control (DAC), they are synonymous.

Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC or RBAC) are types of Non Discretionary Access Control (NDAC).

Tip:

When you have two answers that are synonymous they are not the right choice for sure.

There is only one access control model that makes use of Label, Clearances, and Categories, it is Mandatory Access Control, none of the other one makes use of those items.

Reference(s) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION: 184

Which of the following is the best reason for the use of an automated risk analysis tool?

A. Much of the data gathered during the review cannot be reused for subsequent analysis.

B. Automated methodologies require minimal training and knowledge of risk analysis.

C. Most software tools have user interfaces that are easy to use and does not require any training.

D. Information gathering would be minimized and expedited due to the amount of information already built into the tool.

Answer: (SHOW ANSWER)

The use of tools simplifies this process. Not only do they usually have a database of assests, threats, and vulnerabilities but they also speed up the entire process.

Using Automated tools for performing a risk assessment can reduce the time it takes to perform them and can simplify the process as well. The better types of these tools include a well-researched threat population and associated statistics. Using one of these tools virtually ensures that no relevant threat is overlooked, and associated risks are accepted as a consequence of the threat being overlooked.

In most situations, the assessor will turn to the use of a variety of automated tools to assist in the vulnerability assessment process. These tools contain extensive databases of specific known vulnerabilities as well as the ability to analyze system and network configuration information to predict where a particular system might be vulnerable to different types of attacks. There are many different types of tools currently available to address a wide variety of vulnerability assessment needs. Some tools will examine a

system from the viewpoint of the network, seeking to determine if a system can be compromised by a remote attacker exploiting available services on a particular host system. These tools will test for open ports listening for connections, known vulnerabilities in common services, and known operating system exploits.

Michael Gregg says:
Automated tools are available that minimize the effort of the manual process. These programs enable users to rerun the analysis with different parameters to answer "what-ifs." They perform calculations quickly and can be used to estimate future expected losses easier than performing the calculations manually.
Shon Harris in her latest book says:
The gathered data can be reused, greatly reducing the time required to perform subsequent analyses. The risk analysis team can also print reports and comprehensive graphs to present to management.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4655-4661). Auerbach Publications. Kindle Edition.
and
CISSP Exam Cram 2 by Michael Gregg
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 2333-2335). McGraw-Hill. Kindle Edition.
The following answers are incorrect:
Much of the data gathered during the review cannot be reused for subsequent analysis. Is incorrect because the data can be reused for later analysis.
Automated methodologies require minimal training and knowledge of risk analysis. Is incorrect because it is not the best answer. While a minimal amount of training and knowledge is needed, the analysis should still be performed by skilled professionals.
Most software tools have user interfaces that are easy to use and does not require any training. Is incorrect because it is not the best answer. While many of the user interfaces are easy to use it is better if the tool already has information built into it. There is always a training curve when any product is being used for the first time.

NEW QUESTION: 185
Which of the following is NOT a type of motion detector?
A. Photoelectric sensor
B. Passive infrared sensors
C. Microwave Sensor.
D. Ultrasonic Sensor.
Answer: A (LEAVE A REPLY)
A photoelectric sensor does not "directly" sense motion there is a narrow
beam that won't set off the sensor unless the beam is broken. Photoelectric sensors, along with dry contact switches, are a type of perimeter intrusion detector.
All of the other answers are valid types of motion detectors types.
The content below on the different types of sensors is from Wikepedia:

Indoor Sensors

These types of sensors are designed for indoor use. Outdoor use would not be advised due to false alarm vulnerability and weather durability.Passive infrared detectors

Passive Infrared Sensor

The passive infrared detector (PIR) is one of the most common detectors found in household and small business environments because it offers affordable and reliable functionality. The term passive means the detector is able to function without the need to generate and radiate its own energy (unlike ultrasonic and microwave volumetric intrusion detectors that are "active" in operation). PIRs are able to distinguish if an infrared emitting object is present by first learning the ambient temperature of the monitored space and then detecting a change in the temperature caused by the presence of an object. Using the principle of differentiation, which is a check of presence or nonpresence, PIRs verify if an intruder or object is actually there. Creating individual zones of detection where each zone comprises one or more layers can achieve differentiation. Between the zones there are areas of no sensitivity (dead zones) that are used by the sensor for comparison.

Ultrasonic detectors

Using frequencies between 15 kHz and 75 kHz, these active detectors transmit ultrasonic sound waves that are inaudible to humans. The Doppler shift principle is the underlying method of operation, in which a change in frequency is detected due to object motion. This is caused when a moving object changes the frequency of sound waves around it. Two conditions must occur to successfully detect a Doppler shift event:

There must be motion of an object either towards or away from the receiver.

The motion of the object must cause a change in the ultrasonic frequency to the receiver relative to the transmitting frequency.

The ultrasonic detector operates by the transmitter emitting an ultrasonic signal into the area to be protected. The sound waves are reflected by solid objects (such as the surrounding floor, walls and ceiling) and then detected by the receiver. Because ultrasonic waves are transmitted through air, then hard-surfaced objects tend to reflect most of the ultrasonic energy, while soft surfaces tend to absorb most energy.

When the surfaces are stationary, the frequency of the waves detected by the receiver will be equal to the transmitted frequency. However, a change in frequency will occur as a result of the Doppler principle, when a person or object is moving towards or away from the detector. Such an event initiates an alarm signal. This technology is considered obsolete by many alarm professionals, and is not actively installed.

Microwave detectors This device emits microwaves from a transmitter and detects any reflected microwaves or reduction in beam intensity using a receiver. The transmitter and receiver are usually combined inside a single housing (monostatic) for indoor applications, and separate housings (bistatic) for outdoor applications. To reduce false alarms this type of detector is usually combined with a passive infrared detector or "Dualtec" alarm.

Microwave detectors respond to a Doppler shift in the frequency of the reflected energy, by a phase shift, or by a sudden reduction of the level of received energy. Any of these effects may indicate motion of an intruder. Photo-electric beams Photoelectric beam systems detect the presence of an intruder by

transmitting visible or infrared light beams across an area, where these beams may be obstructed. To improve the detection surface area, the beams are often employed in stacks of two or more. However, if an intruder is aware of the technology's presence, it can be avoided. The technology can be an effective long-range detection system, if installed in stacks of three or more where the transmitters and receivers are staggered to create a fence-like barrier. Systems are available for both internal and external applications. To prevent a clandestine attack using a secondary light source being used to hold the detector in a 'sealed' condition whilst an intruder passes through, most systems use and detect a modulated light source.
Glass break detectors The glass break detector may be used for internal perimeter building protection. When glass breaks it generates sound in a wide band of frequencies. These can range from infrasonic, which is below 20 hertz (Hz) and can not be heard by the human ear, through the audio band from 20 Hz to 20 kHz which humans can hear, right up to ultrasonic, which is above 20 kHz and again cannot be heard. Glass break acoustic detectors are mounted in close proximity to the glass panes and listen for sound frequencies associated with glass breaking. Seismic glass break detectors are different in that they are installed on the glass pane. When glass breaks it produces specific shock frequencies which travel through the glass and often through the window frame and the surrounding walls and ceiling. Typically, the most intense frequencies generated are between 3 and 5 kHz, depending on the type of glass and the presence of a plastic interlayer. Seismic glass break detectors "feel" these shock frequencies and in turn generate an alarm condition.
The more primitive detection method involves gluing a thin strip of conducting foil on the inside of the glass and putting low-power electrical current through it. Breaking the glass is practically guaranteed to tear the foil and break the circuit. Smoke, heat, and carbon monoxide detectors
Heat Detection System Most systems may also be equipped with smoke, heat, and/or carbon monoxide detectors. These are also known as 24 hour zones (which are on at all times). Smoke detectors and heat detectors protect from the risk of fire and carbon monoxide detectors protect from the risk of carbon monoxide. Although an intruder alarm panel may also have these detectors connected, it may not meet all the local fire code requirements of a fire alarm system.
Other types of volumetric sensors could be:
Active Infrared Passive Infrared/Microware combined Radar Accoustical Sensor/Audio Vibration Sensor (seismic) Air Turbulence

NEW QUESTION: 186
Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:
A. through access control mechanisms that require identification and authentication and through the audit function.
B. through logical or technical controls involving the restriction of access to systems and the protection of information.
C. through logical or technical controls but not involving the restriction of access to systems and the protection of information.

D. through access control mechanisms that do not require identification and authentication and do not operate through the audit function.

Answer: A (LEAVE A REPLY)

Section: Access Control

Explanation/Reference:

Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 187

Which of the following statements pertaining to protection rings is false?

A. They provide strict boundaries and definitions on what the processes that work within each ring can access.

B. Programs operating in inner rings are usually referred to as existing in a privileged mode.

C. They support the CIA triad requirements of multitasking operating systems.

D. They provide users with a direct access to peripherals

Answer: D (LEAVE A REPLY)

In computer science, hierarchical protection domains, often called protection rings, are mechanisms to protect data and functionality from faults (fault tolerance) and malicious behaviour (computer security). This approach is diametrically opposite to that of capability-based security.

Computer operating systems provide different levels of access to resources. A protection ring is one of two or more hierarchical levels or layers of privilege within the architecture of a computer system. This is generally hardware-enforced by some CPU architectures that
provide different CPU modes at the hardware or microcode level.

Rings are arranged in a hierarchy from most privileged (most trusted, usually numbered zero) to least privileged (least trusted, usually with the highest ring number). On most operating systems, Ring 0 is the level with the most privileges and interacts most directly with the physical hardware such as the CPU and memory.

Special gates between rings are provided to allow an outer ring to access an inner ring's resources in a predefined manner, as opposed to allowing arbitrary usage. Correctly gating access between rings can improve security by preventing programs from one ring or privilege level from misusing resources intended for programs in another. For example, spyware running as a user program in Ring 3 should be prevented from turning on a web camera without informing the user, since hardware access should be a Ring 1 function reserved for device drivers. Programs such as web browsers running in higher numbered rings must request access to the network, a resource restricted to a lower numbered ring.

"They provide strict boundaries and definitions on what the processes that work within each

ring can access" is incorrect. This is in fact one of the characteristics of a ring protection system.
"Programs operating in inner rings are usually referred to as existing in a privileged mode" is incorrect. This is in fact one of the characteristics of a ring protection system.
"They support the CIA triad requirements of multitasking operating systems" is incorrect. This is in fact one of the characteristics of a ring protection system.
Reference(s) used for this question:
CBK, pp. 310-311
AIO3, pp. 253-256
AIOv4 Security Architecture and Design (pages 308 - 310)
AIOv5 Security Architecture and Design (pages 309 - 312)

NEW QUESTION: 188
Which of the following rules pertaining to a Business Continuity Plan/Disaster Recovery Plan is incorrect?
A. In order to facilitate recovery, a single plan should cover all locations.
B. There should be requirements to form a committee to decide a course of action. These decisions should be made ahead of time and incorporated into the plan.
C. In its procedures and tasks, the plan should refer to functions, not specific individuals.
D. Critical vendors should be contacted ahead of time to validate equipment can be obtained in a timely manner.
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The first documentation rule when it comes to a BCP/DRP is "one plan, one building". Much of the plan revolves around reconstructing a facility and replenishing it with production contents. If more than one facility is involved, then the reader of the plan will find it difficult to identify quantities and specifications of replacement resource items. It is possible to have multiple plans for a single building, but those plans must be linked so that the identification and ordering of resource items is centralized. All other statements are correct.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 162).

NEW QUESTION: 189
Which of the following is NOT a type of motion detector?
A. Photoelectric sensor
B. Passive infrared sensors
C. Microwave Sensor.
D. Ultrasonic Sensor.
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:

A photoelectric sensor does not "directly" sense motion there is a narrow beam that won't set off the sensor unless the beam is broken. Photoelectric sensors, along with dry contact switches, are a type of perimeter intrusion detector.
All of the other answers are valid types of motion detectors types.
The content below on the different types of sensors is from Wikepedia:
Indoor Sensors
These types of sensors are designed for indoor use. Outdoor use would not be advised due to false alarm vulnerability and weather durability.Passive infrared detectors
Passive Infrared Sensor
The passive infrared detector (PIR) is one of the most common detectors found in household and small business environments because it offers affordable and reliable functionality. The term passive means the detector is able to function without the need to generate and radiate its own energy (unlike ultrasonic and microwave volumetric intrusion detectors that are "active" in operation). PIRs are able to distinguish if an infrared emitting object is present by first learning the ambient temperature of the monitored space and then detecting a change in the temperature caused by the presence of an object. Using the principle of differentiation, which is a check of presence or nonpresence, PIRs verify if an intruder or object is actually there. Creating individual zones of detection where each zone comprises one or more layers can achieve differentiation. Between the zones there are areas of no sensitivity (dead zones) that are used by the sensor for comparison.
Ultrasonic detectors
Using frequencies between 15 kHz and 75 kHz, these active detectors transmit ultrasonic sound waves that are inaudible to humans. The Doppler shift principle is the underlying method of operation, in which a change in frequency is detected due to object motion. This is caused when a moving object changes the frequency of sound waves around it. Two conditions must occur to successfully detect a Doppler shift event:
There must be motion of an object either towards or away from the receiver.
The motion of the object must cause a change in the ultrasonic frequency to the receiver relative to the transmitting frequency.
The ultrasonic detector operates by the transmitter emitting an ultrasonic signal into the area to be protected.
The sound waves are reflected by solid objects (such as the surrounding floor, walls and ceiling) and then detected by the receiver. Because ultrasonic waves are transmitted through air, then hard-surfaced objects tend to reflect most of the ultrasonic energy, while soft surfaces tend to absorb most energy. When the surfaces are stationary, the frequency of the waves detected by the receiver will be equal to the transmitted frequency. However, a change in frequency will occur as a result of the Doppler principle, when a person or object is moving towards or away from the detector. Such an event initiates an alarm signal. This technology is considered obsolete by many alarm professionals, and is not actively installed.
Microwave detectors
This device emits microwaves from a transmitter and detects any reflected microwaves or reduction in beam intensity using a receiver. The transmitter and receiver are usually combined inside a single housing (monostatic) for indoor applications, and separate housings (bistatic) for outdoor applications. To

reduce false alarms this type of detector is usually combined with a passive infrared detector or "Dualtec" alarm.

Microwave detectors respond to a Doppler shift in the frequency of the reflected energy, by a phase shift, or by a sudden reduction of the level of received energy. Any of these effects may indicate motion of an intruder.

Photo-electric beams

Photoelectric beam systems detect the presence of an intruder by transmitting visible or infrared light beams across an area, where these beams may be obstructed. To improve the detection surface area, the beams are often employed in stacks of two or more. However, if an intruder is aware of the technology's presence, it can be avoided. The technology can be an effective long-range detection system, if installed in stacks of three or more where the transmitters and receivers are staggered to create a fence-like barrier. Systems are available for both internal and external applications. To prevent a clandestine attack using a secondary light source being used to hold the detector in a 'sealed' condition whilst an intruder passes through, most systems use and detect a modulated light source.

Glass break detectors

The glass break detector may be used for internal perimeter building protection. When glass breaks it generates sound in a wide band of frequencies. These can range from infrasonic, which is below 20 hertz (Hz) and can not be heard by the human ear, through the audio band from 20 Hz to 20 kHz which humans can hear, right up to ultrasonic, which is above 20 kHz and again cannot be heard. Glass break acoustic detectors are mounted in close proximity to the glass panes and listen for sound frequencies associated with glass breaking.

Seismic glass break detectors are different in that they are installed on the glass pane. When glass breaks it produces specific shock frequencies which travel through the glass and often through the window frame and the surrounding walls and ceiling. Typically, the most intense frequencies generated are between 3 and 5 kHz, depending on the type of glass and the presence of a plastic interlayer. Seismic glass break detectors "feel" these shock frequencies and in turn generate an alarm condition. The more primitive detection method involves gluing a thin strip of conducting foil on the inside of the glass and putting low-power electrical current through it. Breaking the glass is practically guaranteed to tear the foil and break the circuit.

Smoke, heat, and carbon monoxide detectors

Heat Detection System

Most systems may also be equipped with smoke, heat, and/or carbon monoxide detectors. These are also known as 24 hour zones (which are on at all times). Smoke detectors and heat detectors protect from the risk of fire and carbon monoxide detectors protect from the risk of carbon monoxide. Although an intruder alarm panel may also have these detectors connected, it may not meet all the local fire code requirements of a fire alarm system.

Other types of volumetric sensors could be:

Active Infrared

Passive Infrared/Microware combined

Radar

Accoustical Sensor/Audio

Vibration Sensor (seismic)
Air Turbulence

NEW QUESTION: 190
Which of the following is an example of an active attack?
A. Traffic analysis
B. Scanning
C. Eavesdropping
D. Wiretapping
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Scanning is definitively a very active attack. The attacker will make use of a scanner to perform the attack, the scanner will send a very large quantity of packets to the target in order to illicit responses that allows the attacker to find information about the operating system, vulnerabilities, misconfiguration and more. The packets being sent are sometimes attempting to identify if a known vulnerability exist on the remote hosts.
A passive attack is usually done in the footprinting phase of an attack. While doing your passive reconnaissance you never send a single packet to the destination target. You gather information from public databases such as the DNS servers, public information through search engines, financial information from finance web sites, and technical infomation from mailing list archive or job posting for example.
An attack can be active or passive.
An "active attack" attempts to alter system resources or affect their operation.
A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. (E.g., see: wiretapping.) The following are all incorrect answers because they are all passive attacks:
Traffic Analysis - Is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security.
Eavesdropping - Eavesdropping is another security risk posed to networks. Because of the way some networks are built, anything that gets sent out is broadcast to everyone. Under normal circumstances, only the computer that the data was meant for will process that information. However, hackers can set up programs on their computers called "sniffers" that capture all data being broadcast over the network. By carefully examining the data, hackers can often reconstruct real data that was never meant for them. Some of the most damaging things that get sniffed include passwords and credit card information.
In the cryptographic context, Eavesdropping and sniffing data as it passes over a network are considered passive attacks because the attacker is not affecting the protocol, algorithm, key, message, or any parts of the encryption system. Passive attacks are hard to detect, so in most cases methods are put in place

to try to prevent them rather than to detect and stop them. Altering messages, modifying system files, and masquerading as another individual are acts that are considered active attacks because the attacker is actually doing something instead of sitting back and gathering data. Passive attacks are usually used to gain information prior to carrying out an active attack." Wiretapping - Wiretapping refers to listening in on electronic communications on telephones, computers, and other devices. Many governments use it as a law enforcement tool, and it is also used in fields like corporate espionage to gain access to privileged information. Depending on where in the world one is, wiretapping may be tightly controlled with laws that are designed to protect privacy rights, or it may be a widely accepted practice with little or no protections for citizens. Several advocacy organizations have been established to help civilians understand these laws in their areas, and to fight illegal wiretapping.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 6th Edition, Cryptography, Page 865 and
http://en.wikipedia.org/wiki/Attack_%28computing%29
and
http://www.wisegeek.com/what-is-wiretapping.htm
and
https://pangea.stanford.edu/computing/resources/network/security/risks.php and
http://en.wikipedia.org/wiki/Traffic_analysis

NEW QUESTION: 191
What is called a system that is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it?
A. A fail safe system
B. A fail soft system
C. A fault-tolerant system
D. A failover system
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
A fault-tolerant system is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it. In a fail-safe system, program execution is terminated, and the system is protected from being compromised when a hardware or software failure occurs and is detected. In a fail-soft system, when a hardware or software failure occurs and is detected, selected, non-critical processing is terminated. The term failover refers to switching to a duplicate "hot" backup component in real-time when a hardware or software failure occurs, enabling processing to continue.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 196).

NEW QUESTION: 192
Some Unix systems use a very simple cipher called _____.
A. SOT14

B. Block
C. ROT13
D. DES
E. Stream
Answer: C (LEAVE A REPLY)

NEW QUESTION: 193
Which of the following tools is NOT likely to be used by a hacker?
A. Nessus
B. Saint
C. Tripwire
D. Nmap
Answer: C (LEAVE A REPLY)
Explanation/Reference:
It is a data integrity assurance software aimed at detecting and reporting accidental or malicious changes to data.
The following answers are incorrect :
Nessus is incorrect as it is a vulnerability scanner used by hackers in discovering vulnerabilities in a system.
Saint is also incorrect as it is also a network vulnerability scanner likely to be used by hackers.
Nmap is also incorrect as it is a port scanner for network exploration and likely to be used by hackers.
Reference :
Tripwire : http://www.tripwire.com
Nessus : http://www.nessus.org
Saint : http://www.saintcorporation.com/saint
Nmap : http://insecure.org/nmap

NEW QUESTION: 194
Which of the following is NOT a common integrity goal?
A. Prevent unauthorized users from making modifications.
B. Maintain internal and external consistency.
C. Prevent authorized users from making improper modifications.
D. Prevent paths that could lead to inappropriate disclosure.
Answer: (SHOW ANSWER)
Inappropriate disclosure is a confidentiality, not an integrity goal.
All of the other choices above are integrity goals addressed by the Clark-Wilson integrity model.
The Clark-Wilson model is an integrity model that addresses all three integrity goals:
1.prevent unauthorized users from making modifications,
2.prevent authorized users from making improper modifications, and
3.maintain internal and external consistency through auditing.

NOTE: Biba address only the first goal of integrity above
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1384). McGraw-Hill. Kindle Edition.

NEW QUESTION: 195
Notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects is part of:
A. Incident Evaluation
B. Incident Recognition
C. Incident Protection
D. Incident Response
Answer: D (LEAVE A REPLY)
Explanation/Reference:
These are core functions of the incident response process.
"Incident Evaluation" is incorrect. Evaluation of the extent and cause of the incident is a component of the incident response process.
"Incident Recognition" is incorrect. Recognition that an incident has occurred is the precursor to the initiation of the incident response process.
"Incident Protection" is incorrect. This is an almost-right-sounding nonsense answer to distract the unwary.
References
CBK, pp. 698 - 703

NEW QUESTION: 196
Which of the following is NOT true concerning Application Control?
A. It limits end users use of applications in such a way that only particular screens are visible.
B. Only specific records can be requested through the application controls
C. Particular usage of the application can be recorded for audit purposes
D. It is non-transparent to the endpoint applications so changes are needed to the applications and databases involved
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, Auerbach.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP

exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 197
A packet containing a long string of NOP's followed by a command is usually indicative of what?
A. A syn scan.
B. A half-port scan.
C. A buffer overflow attack.
D. A packet destined for the network's broadcast address.
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
A series of the same control, hexidecimal, characters imbedded in the string is usually an indicator of a buffer overflow attack. A NOP is a instruction which does nothing (No Operation - the hexadecimal equivalent is
0x90)
The following answers are incorrect:
A syn scan. This is incorrect because a SYN scan is when a SYN packet is sent to a specific port and the results are then analyzed.
A half-port scan. This is incorrect because the port scanner generates a SYN packet. If the target port is open, it will respond with a SYN-ACK packet. The scanner host responds with a RST packet, closing the connection before the handshake is completed. Also known as a Half Open Port scan.
A packet destined for the network's broadcast address. This is incorrect because this type of packet would not contain a long string of NOP characters.

NEW QUESTION: 198
Which of the following test makes sure the modified or new system includes appropriate access controls and does not introduce any security holes that might compromise other systems?
A. Recovery testing
B. Security testing
C. Stress/volume testing
D. Interface testing
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Security testing makes sure the modified or new system includes appropriate access controls and does not introduce any security holes that might compromise other systems.
Recovery testing checks the system's ability to recover after a software or hardware failure.
Stress/volume testing involves testing an application with large quantities of data in order to evaluate performance during peak hours.

Interface testing evaluates the connection of two or more components that pass information from one area to another.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).

NEW QUESTION: 199
Which of the following statements is true about data encryption as a method of protecting data?
A. It should sometimes be used for password files
B. It is usually easily administered
C. It makes few demands on system resources
D. It requires careful key management
Answer: D (LEAVE A REPLY)
In cryptography, you always assume the "bad guy" has the encryption algorithm (indeed, many algorithms such as DES, Triple DES, AES, etc. are public domain). What the bad guy lacks is the key used to complete that algorithm and encrypt/decrypt information. Therefore, protection of the key, controlled distribution, scheduled key change, timely destruction, and several other factors require careful consideration. All of these factors are covered under the umbrella term of "key management".
Another significant consideration is the case of "data encryption as a method of protecting data" as the question states. If that data is to be stored over a long period of time (such as on backup), you must ensure that your key management scheme stores old keys for as long as they will be needed to decrypt the information they encrypted.
The other answers are not correct because:
"It should sometimes be used for password files." - Encryption is often used to encrypt passwords stored within password files, but it is not typically effective for the password file itself. On most systems, if a user cannot access the contents of a password file, they cannot authenticate. Encrypting the entire file prevents that access.
"It is usually easily administered." - Developments over the last several years have made cryptography significantly easier to manage and administer. But it remains a significant challenge. This is not a good answer.
"It makes few demands on system resources." - Cryptography is, essentially, a large complex mathematical algorithm. In order to encrypt and decrypt information, the system must perform this algorithm hundreds, thousands, or even millions/billions/trillions of times. This becomes system resource intensive, making this a very bad answer.
Reference:
Official ISC2 Guide page: 266 (poor explanation)
All in One Third Edition page: 657 (excellent explanation)
Key Management - Page 732, All in One Fourth Edition

NEW QUESTION: 200
What is a packet sniffer?

A. It tracks network connections to off-site locations.
B. It monitors network traffic for illegal packets.
C. It scans network segments for cabling faults.
D. It captures network traffic for later analysis.
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 201
What are the three most important functions that Digital Signatures perform?
A. Integrity, Confidentiality and Authorization
B. Integrity, Authentication and Nonrepudiation
C. Authorization, Authentication and Nonrepudiation
D. Authorization, Detection and Accountability
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2.

NEW QUESTION: 202
What algorithm was DES derived from?
A. Twofish.
B. Skipjack.
C. Brooks-Aldeman.
D. Lucifer.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
NSA took the 128-bit algorithm Lucifer that IBM developed, reduced the key size to 64 bits and with that developed DES.
The following answers are incorrect:
Twofish. This is incorrect because Twofish is related to Blowfish as a possible replacement for DES.
Skipjack. This is incorrect, Skipjack was developed after DES by the NSA .
Brooks-Aldeman. This is incorrect because this is a distractor, no algorithm exists with this name.

NEW QUESTION: 203
Good security is built on which of the following concept?
A. The concept of a pass-through device that only allows certain traffic in and out
B. The Concept of defense in depth
C. The Concept of Preventative controls
D. The Concept of Defensive Controls

Answer: B (LEAVE A REPLY)
Explanation/Reference:
This the best of the four answers as a defense that depends on multiple layers is superior to one where all protection is embedded in a single layer (e.g., a firewall). Defense in depth would include all categories of controls.
The Following answers are incorrect:
"Concept of a pass through device that only allows certain traffic in and out" is incorrect. This is one definition of a firewall which can be a component of a defense in depth strategy in combination with other measures.
"Concept of preventative controls" is incorrect. This is a component of a defense in depth strategy but the core concept is that there must be multiple layers of defenses.
"Concept of defensive controls" is incorrect. This is a component of a defense in depth strategy but the core concept is that there must be multiple layers of defenses.
References:
http://en.wikipedia.org/wiki/Defense_in_depth_(computing)
http://www.nsa.gov/snac/support/defenseindepth.pdf

NEW QUESTION: 204
What is the PRIMARY goal of incident handling?
A. Successfully retrieve all evidence that can be used to prosecute
B. Improve the company's ability to be prepared for threats and disasters
C. Improve the company's disaster recovery plan
D. Contain and repair any damage caused by an event.
Answer: D (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
This is the PRIMARY goal of an incident handling process.
The other answers are incorrect because :
Successfully retrieve all evidence that can be used to prosecute is more often used in identifying weaknesses than in prosecuting.
Improve the company's ability to be prepared for threats and disasters is more appropriate for a disaster recovery plan.
Improve the company's disaster recovery plan is also more appropriate for disaster recovery plan.
Reference : Shon Harris AIO v3 , Chapter - 10 : Law, Investigation, and Ethics , Page : 727-728

NEW QUESTION: 205
Which of the following tools is NOT likely to be used by a hacker?
A. Nessus
B. Saint
C. Tripwire
D. Nmap

Answer: C (LEAVE A REPLY)

It is a data integrity assurance software aimed at detecting and reporting accidental or malicious changes to data.

The following answers are incorrect :

Nessus is incorrect as it is a vulnerability scanner used by hackers in discovering vulnerabilities in a system.

Saint is also incorrect as it is also a network vulnerability scanner likely to be used by hackers.

Nmap is also incorrect as it is a port scanner for network exploration and likely to be used by hackers.

Reference :

Tripwire : http://www.tripwire.com

Nessus : http://www.nessus.org

Saint : http://www.saintcorporation.com/saint

Nmap : http://insecure.org/nmap

NEW QUESTION: 206

What is the difference between Advisory and Regulatory security policies?

A. there is no difference between them

B. regulatory policies are high level policy, while advisory policies are very detailed

C. Advisory policies are not mandated. Regulatory policies must be implemented.

D. Advisory policies are mandated while Regulatory policies are not

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Advisory policies are security polices that are not mandated to be followed but are strongly suggested, perhaps with serious consequences defined for failure to follow them (such as termination, a job action warning, and so forth). A company with such policies wants most employees to consider these policies mandatory.

Most policies fall under this broad category.

Advisory policies can have many exclusions or application levels. Thus, these policies can control some employees more than others, according to their roles and responsibilities within that organization. For example, a policy that

requires a certain procedure for transaction processing might allow for an alternative procedure under certain, specified conditions.

Regulatory

Regulatory policies are security policies that an organization must implement due to compliance, regulation, or other legal requirements. These companies might be financial institutions, public utilities, or some other type of organization that operates in the public interest. These policies are usually very detailed and are specific to the industry in which the organization operates.

Regulatory polices commonly have two main purposes:

1. To ensure that an organization is following the standard procedures or base practices of operation in its specific industry
2. To give an organization the confidence that it is following the standard and accepted industry policy
Informative
Informative policies are policies that exist simply to inform the reader. There are no implied or specified requirements, and the audience for this information could be certain internal (within the organization) or external parties. This does not mean that the policies are authorized for public consumption but that they are general enough to be distributed to external parties (vendors accessing an extranet, for example) without a loss of confidentiality.
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 12, Chapter 1: Security Management Practices.
also see:
The CISSP Prep Guide:Mastering the Ten Domains of Computer Security by Ronald L. Krutz, Russell Dean Vines, Edward M. Stroz
also see:
http://i-data-recovery.com/information-security/information-security-policies-standards-guidelines-and-procedures

NEW QUESTION: 207
What attribute is included in a X.509-certificate?
A. Distinguished name of the subject
B. Telephone number of the department
C. secret key of the issuing CA
D. the key pair of the certificate holder
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile; GUTMANN, P., X.509 style guide; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

NEW QUESTION: 208
Who is ultimately responsible for the security of computer based information systems within an organization?
A. The tech support team
B. The Operation Team.
C. The management team.
D. The training team.
Answer: C (LEAVE A REPLY)
Explanation/Reference:

If there is no support by management to implement, execute, and enforce security policies and procedure, then they won't work. Senior management must be involved in this because they have an obligation to the organization to protect the assests . The requirement here is for management to show "due diligence" in establishing an effective compliance, or security program.
The following answers are incorrect:
The tech support team. Is incorrect because the ultimate responsibility is with management for the security of computer-based information systems.
The Operation Team. Is incorrect because the ultimate responsibility is with management for the security of computer-based information systems.
The Training Team. Is incorrect because the ultimate responsibility is with management for the security of computer-based information systems.
Reference(s) used for this question:
OIG CBK Information Security Management and Risk Management (page 20 - 22)

NEW QUESTION: 209
What protocol is used to match an IP address to the appropriate hardware address of the packet's destination so it can be sent?
A. Routing tables
B. Address resolution protocol (ARP)
C. Reverse address resolution protocol (RARP)
D. Internet Control Message Protocol (ICMP)
Answer: B (LEAVE A REPLY)
Explanation/Reference:
The Address Resolution Protocol (ARP) is used to match an IP address to an Ethernet address so the packet can be sent to the appropriate node.
Shon Harris in her book says:
MAC and IP addresses must be properly mapped so they can be correctly resolved. This happens through the Address Resolution Protocol (ARP). When the data link layer receives a frame, the network layer has already attached the destination IP address to it, but the data link layer cannot understand the IP address and thus invokes ARP for help.
ARP broadcasts a frame requesting the MAC address that corresponds with the destination IP address. Each computer on the subnet receives this broadcast frame, and all but the computer that has the requested IP address ignore it.
The computer that has the destination IP address responds with its MAC address. Now ARP knows what hardware address corresponds with that specific IP address. The data link layer takes the frame, adds the hardware address to it, and passes it on to the physical layer, which enables the frame to hit the wire and go to the destination computer.
ARP maps the hardware address and associated IP address and stores this mapping in its table for a predefined amount of time. This caching is done so that when another frame destined for the same IP address needs to hit the wire, ARP does not need to broadcast its request again. It just looks in its table for this information.

Man-In-The-Middle attack
Because ARP does not require authentication, an attacker could place bogus entries into the ARP cache of a remote host (gratuitous ARP replies) to carry out attacks, such as a man-in-the-middle attacks. This attack is called ARP poisoning.
The following answers were incorrect:
RARP is used to match an Ethernet address to an IP address.
ICMP is a management protocol whose function is to send message between network devices.
Routing tables are used by routers to choose the appropriate interface to route packets.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Chapter 6 Telecommunications and Network Security, Pages 580-581 or on the Kindle edition look around Locations 12298-12306. McGraw- Hill. Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK , Third Edition: Telecommunications and Network Security, Page 342.

NEW QUESTION: 210
Which of the following security mode of operation does NOT require all users to have the clearance for all information processed on the system?
A. Compartmented security mode
B. Multilevel security mode
C. System-high security mode
D. Dedicated security mode
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
The multilevel security mode permits two or more classification levels of information to be processed at the same time when all the users do not have the clearance of formal approval to access all the information being processed by the system.
In dedicated security mode, all users have the clearance or authorization and need-to-know to all data processed within the system.
In system-high security mode, all users have a security clearance or authorization to access the information but not necessarily a need-to-know for all the information processed on the system (only some of the data).
In compartmented security mode, all users have the clearance to access all the information processed by the system, but might not have the need-to-know and formal access approval.
Generally, Security modes refer to information systems security modes of operations used in mandatory access control (MAC) systems. Often, these systems contain information at various levels of security classification.
The mode of operation is determined by:
The type of users who will be directly or indirectly accessing the system.

The type of data, including classification levels, compartments, and categories, that are processed on the system.
The type of levels of users, their need to know, and formal access approvals that the users will have.
Dedicated security mode
In this mode of operation, all users must have:
Signed NDA for ALL information on the system.
Proper clearance for ALL information on the system.
Formal access approval for ALL information on the system.
A valid need to know for ALL information on the system.
All users can access ALL data.
System high security mode
In this mode of operation, all users must have:
Signed NDA for ALL information on the system.
Proper clearance for ALL information on the system.
Formal access approval for ALL information on the system.
A valid need to know for SOME information on the system.
All users can access SOME data, based on their need to know.
Compartmented security mode
In this mode of operation, all users must have:
Signed NDA for ALL information on the system.
Proper clearance for ALL information on the system.
Formal access approval for SOME information they will access on the system.
A valid need to know for SOME information on the system.
All users can access SOME data, based on their need to know and formal access approval.
Multilevel security mode
In this mode of operation, all users must have:
Signed NDA for ALL information on the system.
Proper clearance for SOME information on the system.
Formal access approval for SOME information on the system.
A valid need to know for SOME information on the system.
All users can access SOME data, based on their need to know, clearance and formal access approval.
REFERENCES:
WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 6).
and
http://en.wikipedia.org/wiki/Security_Modes

NEW QUESTION: 211
What is the most secure way to dispose of information on a CD-ROM?
A. Sanitizing
B. Physical damage
C. Degaussing

D. Physical destruction

Answer: D (LEAVE A REPLY)

First you have to realize that the question is specifically talking about a CDROM. The information stored on a CDROM is not in electro magnetic format, so a degausser woud be inneffective.

You cannot sanitize a CDROM but you might be able to sanitize a RW/CDROM. A CDROM is a write once device and cannot be overwritten like a hard disk or other magnetic device.

Physical Damage would not be enough as information could still be extracted in a lab from the undamaged portion of the media or even from the pieces after the physical damage has been done.

Physical Destruction using a shredder, your microwave oven, melting it, would be very effective and the best choice for a non magnetic media such as a CDROM. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 212

The Clipper Chip utilizes which concept in public key cryptography?

A. Substitution

B. Key Escrow

C. An undefined algorithm

D. Super strong encryption

Answer: (SHOW ANSWER)

Explanation/Reference:

The Clipper chip is a chipset that was developed and promoted by the U.S. Government as an encryption device to be adopted by telecommunications companies for voice transmission. It was announced in 1993 and by 1996 was entirely defunct.

The heart of the concept was key escrow. In the factory, any new telephone or other device with a Clipper chip would be given a "cryptographic key", that would then be provided to the government in "escrow". If government agencies "established their authority" to listen to a communication, then the password would be given to those government agencies, who could then decrypt all data transmitted by that particular telephone.

The CISSP Prep Guide states, "The idea is to divide the key into two parts, and to escrow two portions of the key with two separate 'trusted' organizations. Then, law enforcement officals, after obtaining a court order, can retreive the two pieces of the key from the organizations and decrypt the message."

References:

http://en.wikipedia.org/wiki/Clipper_Chip
and
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 166.

NEW QUESTION: 213
Why is Network File System (NFS) used?
A. It enables two different types of file systems to interoperate.
B. It enables two different types of file systems to share Sun applications.
C. It enables two different types of file systems to use IP/IPX.
D. It enables two different types of file systems to emulate each other.
Answer: A (LEAVE A REPLY)
Network File System (NFS) is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

NEW QUESTION: 214
Which of the following statements pertaining to Asynchronous Transfer Mode (ATM) is false?
A. It can be used for voice
B. it can be used for data
C. It carries various sizes of packets
D. It can be used for video
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
ATM is an example of a fast packet-switching network that can be used for either data, voice or video, but packets are of fixed size.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7:
Telecommunications and Network Security (page 455).

NEW QUESTION: 215
Which layer of the TCP/IP protocol stack corresponds to the ISO/OSI Network layer (layer 3)?
A. Host-to-host layer
B. Internet layer
C. Network access layer
D. Session layer
Answer: B (LEAVE A REPLY)
The Internet layer in the TCP/IP protocol stack corresponds to the network layer (layer 3) in the OSI/ISO model. The host-to-host layer corresponds to the transport layer (layer 4) in the OSI/ISO model. The

Network access layer corresponds to the data link and physical layers (layers 2 and 1) in the OSI/ISO model. The session layer is not defined in the TCP/IP protocol stack.
Source: WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April 2002 (page 1).

NEW QUESTION: 216
CORRECT TEXT
A _____ is a program that can be useful in preventing cookies and Java applets from accessing a system.
Answer:
Firewall

NEW QUESTION: 217
Making sure that only those who are supposed to access the data can access is which of the following?
A. confidentiality.
B. capability.
C. integrity.
D. availability.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
From the published (ISC)2 goals for the Certified Information Systems Security Professional candidate, domain definition. Confidentiality is making sure that only those who are supposed to access the data can access it.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 218
Risk analysis is MOST useful when applied during which phase of the system development process?
A. Project initiation and Planning
B. Functional Requirements definition
C. System Design Specification
D. Development and Implementation
Answer: (SHOW ANSWER)
In most projects the conditions for failure are established at the beginning of the project. Thus risk management should be established at the commencement of the project with a risk assessment during project initiation.
As it is clearly stated in the ISC2 book: Security should be included at the first phase of development and throughout all of the phases of the system development life cycle. This is a key concept to understand for the purpose for the exam.

The most useful time is to undertake it at project initiation, although it is often valuable to update the current risk analysis at later stages.
Attempting to retrofit security after the SDLC is completed would cost a lot more money and might be impossible in some cases. Look at the family of browsers we use today, for the past 8 years they always claim that it is the most secure version that has been released and within days vulnerabilities will be found.
Risks should be monitored throughout the SDLC of the project and reassessed when appropriate.
The phases of the SDLC can very from one source to another one. It could be as simple as Concept, Design, and Implementation. It could also be expanded to include more phases such as this list proposed within the ISC2 Official Study book:
Project Initiation and Planning Functional Requirements Definition System Design Specification Development and Implementation Documentations and Common Program Controls Testing and Evaluation Control, certification and accreditation (C&A) Transition to production (Implementation) And there are two phases that will extend beyond the SDLC, they are:
Operation and Maintenance Support (O&M) Revisions and System Replacement (Disposal)
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 291). and The Official ISC2 Guide to the CISSP CBK , Second Edition, Page 182-185

NEW QUESTION: 219
Which of the following is not a preventive operational control?
A. Protecting laptops, personal computers and workstations.
B. Controlling software viruses.
C. Controlling data media access and disposal.
D. Conducting security awareness and technical training.
Answer: (SHOW ANSWER)
Conducting security awareness and technical training to ensure that end
users and system users are aware of the rules of behaviour and their responsibilities in protecting the organization's mission is an example of a preventive management control, therefore not an operational control.
Source: STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 37).

NEW QUESTION: 220
What is the PRIMARY use of a password?
A. Allow access to files.
B. Identify the user.
C. Authenticate the user.
D. Segregate various user's accesses.
Answer: C (LEAVE A REPLY)
Explanation/Reference:

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 221
Which of the following does not apply to system-generated passwords?
A. Passwords are harder to remember for users.
B. If the password-generating algorithm gets to be known, the entire system is in jeopardy.
C. Passwords are more vulnerable to brute force and dictionary attacks.
D. Passwords are harder to guess for attackers.
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Users tend to choose easier to remember passwords. System-generated passwords can provide stronger, harder to guess passwords. Since they are based on rules provided by the administrator, they can include combinations of uppercase/lowercase letters, numbers and special characters, making them less vulnerable to brute force and dictionary attacks. One danger is that they are also harder to remember for users, who will tend to write them down, making them more vulnerable to anyone having access to the user's desk. Another danger with system-generated passwords is that if the password-generating algorithm gets to be known, the entire system is in jeopardy.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 64).

NEW QUESTION: 222
What would BEST define risk management?
A. The process of eliminating the risk
B. The process of assessing the risks
C. The process of reducing risk to an acceptable level
D. The process of transferring risk
Answer: (SHOW ANSWER)
This is the basic process of risk management.
Risk is the possibility of damage happening and the ramifications of such damage should it occur. Information risk management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.
Proper risk management requires a strong commitment from senior management, a documented process that supports the organization's mission, an information risk management (IRM) policy and a delegated IRM team. Once you've identified your company's acceptable level of risk, you need to develop an information risk management policy.

The IRM policy should be a subset of the organization's overall risk management policy (risks to a company include more than just information security issues) and should be mapped to the organizational security policies, which lay out the acceptable risk and the role of security as a whole in the organization. The IRM policy is focused on risk management while the security policy is very high-level and addresses all aspects of security. The IRM policy should address the following items:

Objectives of IRM team Level of risk the company will accept and what is considered an acceptable risk (as defined in the previous article) Formal processes of risk identification Connection between the IRM policy and the organization's strategic planning processes Responsibilities that fall under IRM and the roles that are to fulfill them Mapping of risk to internal controls Approach for changing staff behaviors and resource allocation in response to risk analysis Mapping of risks to performance targets and budgets Key indicators to monitor the effectiveness of controls Shon Harris provides a 10,000-foot view of the risk management process below: A big question that companies have to deal with is, "What is enough security?" This can be restated as, "What is our acceptable risk level?" These two questions have an inverse relationship. You can't know what constitutes enough security unless you know your necessary baseline risk level.

To set an enterprise-wide acceptable risk level for a company, a few things need to be investigated and understood. A company must understand its federal and state legal requirements, its regulatory requirements, its business drivers and objectives, and it must carry out a risk and threat analysis. (I will dig deeper into formalized risk analysis processes in a later article, but for now we will take a broad approach.) The result of these findings is then used to define the company's acceptable risk level, which is then outlined in security policies, standards, guidelines and procedures.

Although there are different methodologies for enterprise risk management, the core components of any risk analysis is made up of the following:

Identify company assets Assign a value to each asset Identify each asset's vulnerabilities and associated threats Calculate the risk for the identified assets

Once these steps are finished, then the risk analysis team can identify the necessary countermeasures to mitigate the calculated risks, carry out cost/benefit analysis for these countermeasures and report to senior management their findings.

When we look at information security, there are several types of risk a corporation needs to be aware of and address properly. The following items touch on the major categories: Physical damage Fire, water, vandalism, power loss, and natural disasters

Human interaction Accidental or intentional action or inaction that can disrupt productivity

Equipment malfunction Failure of systems and peripheral devices

Inside and outside attacks Hacking, cracking, and attacking

Misuse of data Sharing trade secrets, fraud, espionage, and theft

Loss of data Intentional or unintentional loss of information through destructive means

Application error Computation errors, input errors, and buffer overflows

The following answers are incorrect:

The process of eliminating the risk is not the best answer as risk cannot be totally eliminated.

The process of assessing the risks is also not the best answer.

The process of transferring risk is also not the best answer and is one of the ways of handling a risk after a risk analysis has been performed.
References:
Shon Harris , AIO v3 , Chapter 3: Security Management Practices , Page: 66-68
and
http://searchsecurity.techtarget.com/tip/Understanding-risk

NEW QUESTION: 223
Which of the following models does NOT include data integrity or conflict of interest?
A. Biba
B. Clark-Wilson
C. Bell-LaPadula
D. Brewer-Nash
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Bell LaPadula model (Bell 1975): The granularity of objects and subjects is not predefined, but the model prescribes simple access rights. Based on simple access restrictions the Bell LaPadula model enforces a discretionary access control policy enhanced with mandatory rules. Applications with rigid confidentiality requirements and without strong integrity requirements may properly be modeled.
These simple rights combined with the mandatory rules of the policy considerably restrict the spectrum of applications which can be appropriately modeled.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
Also check:
Proceedings of the IFIP TC11 12th International Conference on Information Security, Samos (Greece), May
1996, On Security Models.

NEW QUESTION: 224
In regards to information classification what is the main responsibility of information (data) owner?
A. determining the data sensitivity or classification level
B. running regular data backups
C. audit the data users
D. periodically check the validity and accuracy of the data
Answer: (SHOW ANSWER)
Explanation/Reference:
Making the determination to decide what level of classification the information requires is the main responsibility of the data owner.
The data owner within classification is a person from Management who has been entrusted with a data set that belong to the company. It could be for example the Chief Financial Officer (CFO) who has been entrusted with all financial date or it could be the Human Resource Director who has been entrusted with

all Human Resource data. The information owner will decide what classification will be applied to the data based on Confidentiality, Integrity, Availability, Criticality, and Sensitivity of the data.
The Custodian is the technical person who will implement the proper classification on objects in accordance with the Data Owner. The custodian DOES NOT decide what classification to apply, it is the Data Owner who will dictate to the Custodian what is the classification to apply.
NOTE:
The term Data Owner is also used within Discretionary Access Control (DAC). Within DAC it means the person who has created an object. For example, if I create a file on my system then I am the owner of the file and I can decide who else could get access to the file. It is left to my discretion. Within DAC access is granted based solely on the Identity of the subject, this is why sometimes DAC is referred to as Identity Based Access Control.
The other choices were not the best answer
Running regular backups is the responsibility of custodian.
Audit the data users is the responsibility of the auditors
Periodically check the validity and accuracy of the data is not one of the data owner responsibility
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 14, Chapter 1: Security Management Practices.

NEW QUESTION: 225
What is the highest amount a company should spend annually on countermeasures for protecting an asset valued at $1,000,000 from a threat that has an annualized rate of occurrence (ARO) of once every five years and an exposure factor (EF) of 30%?
A. $300,000
B. $150,000
C. $60,000
D. $1,500
Answer: C (LEAVE A REPLY)
The cost of a countermeasure should not be greater in cost than the risk it mitigates (ALE). For a quantitative risk assessment, the equation is ALE = ARO x SLE where the SLE is calculated as the product of asset value x exposure factor. An event that happen once every five years would have an ARO of .2 (1 divided by 5).
SLE = Asset Value (AV) x Exposure Fact (EF) SLE = 1,000,000 x .30 = 300,000
ALE = SLE x Annualized Rate of Occurance (ARO) ALE = 300,000 x .2 = 60,000
Know your acronyms: ALE -- Annual loss expectancy ARO -- Annual rate of occurrence SLE -- Single loss expectancy
The following are incorrect answers:
$300,000 is incorrect. See the explanation of the correct answer for the correct calculation. $150,000 is incorrect. See the explanation of the correct answer for the correct calculation. $1,500 is incorrect. See the explanation of the correct answer for the correct calculation.
Reference(s) used for this question:

Mc Graw Hill, Shon Harris, CISSP All In One (AIO) book, Sixth Edition , Pages 87-88 and Official ISC2 Guide to the CISSP Exam, (OIG), Pages 60-61

NEW QUESTION: 226
What is called a system that is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it?
A. A fail safe system
B. A fail soft system
C. A fault-tolerant system
D. A failover system
Answer: C (LEAVE A REPLY)
Explanation/Reference:
A fault-tolerant system is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it. In a fail-safe system, program execution is terminated, and the system is protected from being compromised when a hardware or software failure occurs and is detected. In a fail-soft system, when a hardware or software failure occurs and is detected, selected, non-critical processing is terminated. The term failover refers to switching to a duplicate "hot" backup component in real-time when a hardware or software failure occurs, enabling processing to continue.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 196).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 227
Which of the following services is NOT provided by the digital signature standard (DSS)?
A. Encryption
B. Integrity
C. Digital signature
D. Authentication
Answer: A (LEAVE A REPLY)
DSS provides Integrity, digital signature and Authentication, but does not provide Encryption.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 160).

NEW QUESTION: 228
What is the main focus of the Bell-LaPadula security model?
A. Accountability
B. Integrity
C. Confidentiality
D. Availability
Answer: C (LEAVE A REPLY)
The Bell-LaPadula model is a formal model dealing with confidentiality.
The Bell-LaPadula Model (abbreviated BLP) is a state machine model used for enforcing access control in government and military applications. It was developed by David Elliott Bell and Leonard J. LaPadula, subsequent to strong guidance from Roger R. Schell to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) policy. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g."Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public").
The Bell-LaPadula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. In this formal model, the entities in an information system are divided into subjects and objects.
The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system satisfies the security objectives of the model. The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from one state to another state is defined by transition functions.
A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.
The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:
The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).
The -property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The -property is also known as the Confinement property. The Discretionary Security Property - use of an access matrix to specify the discretionary access control.
The following are incorrect answers:
Accountability is incorrect. Accountability requires that actions be traceable to the user that performed them and is not addressed by the Bell-LaPadula model.
Integrity is incorrect. Integrity is addressed in the Biba model rather than Bell-Lapadula.
Availability is incorrect. Availability is concerned with assuring that data/services are

available to authorized users as specified in service level objectives and is not addressed by the Bell-Lapadula model.
References:
CBK, pp. 325-326
AIO3, pp. 279 - 284
AIOv4 Security Architecture and Design (pages 333 - 336)
AIOv5 Security Architecture and Design (pages 336 - 338)
Wikipedia at https://en.wikipedia.org/wiki/Bell-La_Padula_model

NEW QUESTION: 229
Which authentication technique best protects against hijacking?
A. Static authentication
B. Continuous authentication
C. Robust authentication
D. Strong authentication
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
A continuous authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. This is the best protection against hijacking. Static authentication is the type of authentication provided by traditional password schemes and the strength of the authentication is highly dependent on the difficulty of guessing passwords. The robust authentication mechanism relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, and it does not protect against hijacking. Strong authentication refers to a two-factor authentication (like something a user knows and something a user is).
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3: Secured Connections to External Networks (page 51).

NEW QUESTION: 230
Which of the following is an unintended communication path that is NOT protected by the system's normal security mechanisms?
A. A trusted path
B. A protection domain
C. A covert channel
D. A maintenance hook
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
A covert channel is an unintended communication path within a system, therefore it is not protected by the system's normal security mechanisms. Covert channels are a secret way to convey information.

Covert channels are addressed from TCSEC level B2.
The following are incorrect answers:
A trusted path is the protected channel that allows a user to access the Trusted Computing Base (TCB) without being compromised by other processes or users.
A protection domain consists of the execution and memory space assigned to each process.
A maintenance hook is a hardware or software mechanism that was installed to permit system maintenance and to bypass the system's security protections.
Reference used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 6: Operations Security (page 219).

NEW QUESTION: 231
The _____ protocol converts IP addresses (logical) to MAC Addresses (physical)
A. IPSEC
B. DARP
C. DNS
D. ARP
E. None of the above
Answer: (SHOW ANSWER)

NEW QUESTION: 232
Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys. This protocol establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis?
A. Internet Security Association and Key Management Protocol (ISAKMP)
B. Simple Key-management for Internet Protocols (SKIP)
C. Diffie-Hellman Key Distribution Protocol
D. IPsec Key exchange (IKE)
Answer: B (LEAVE A REPLY)
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines Simple Key Management for Internet Protocols (SKIP) as:
A key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.
SKIP is an hybrid Key distribution protocol similar to SSL, except that it establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis. Therefore, no connection setup overhead exists and new keys values are not continually generated.
SKIP uses the knowledge of its own secret key or private component and the destination's public component to calculate a unique key that can only be used between them.
IKE stand for Internet Key Exchange, it makes use of ISAKMP and OAKLEY internally.

Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication and a Diffie-Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.
The following are incorrect answers:
ISAKMP is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.
IKE is an Internet, IPsec, key-establishment protocol (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.
IPsec Key exchange (IKE) is only a detracto.
Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol and
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol

NEW QUESTION: 233
A trusted system does NOT involve which of the following?
A. Enforcement of a security policy.
B. Sufficiency and effectiveness of mechanisms to be able to enforce a security policy.
C. Assurance that the security policy can be enforced in an efficient and reliable manner.
D. Independently-verifiable evidence that the security policy-enforcing mechanisms are sufficient and effective.
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
A trusted system is one that meets its intended security requirements. It involves sufficiency and effectiveness, not necessarily efficiency, in enforcing a security policy. Put succinctly, trusted systems have (1) policy, (2) mechanism, and (3) assurance.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION: 234
Unclassified, Private, Confidential, Secret, Top Secret, and Internal Use Only are levels of
A. Security Classification
B. Object Classification
C. Change Control Classification
D. Data Classification
Answer: D (LEAVE A REPLY)

NEW QUESTION: 235
This free (for personal use) program is used to encrypt and decrypt emails.
A. SHA-1
B. DES
C. PGP
D. 3DES
E. None of the above
F. MD5
Answer: (SHOW ANSWER)

NEW QUESTION: 236
One of these statements about the key elements of a good configuration process is NOT true
A. Accommodate the reuse of proven standards and best practices
B. Ensure that all requirements remain clear, concise, and valid
C. Control modifications to system hardware in order to prevent resource changes
D. Ensure changes, standards, and requirements are communicated promptly and precisely
Answer: (SHOW ANSWER)
Explanation/Reference:
Configuration management isn't about preventing change but ensuring the integrity of IT resources by preventing unauthorised or improper changes.
According to the Official ISC2 guide to the CISSP exam, a good CM process is one that can:
(1) accommodate change;
(2) accommodate the reuse of proven standards and best practices;
(3) ensure that all requirements remain clear, concise, and valid;
(4) ensure changes, standards, and requirements are communicated promptly and precisely; and (5) ensure that the results conform to each instance of the product.
Configuration management
Configuration management (CM) is the detailed recording and updating of information that describes an enterprise's computer systems and networks, including all hardware and software components. Such information typically includes the versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. Special configuration management software is available. When a system needs a hardware or software upgrade, a computer technician can accesses the configuration management program and database to see what is currently installed. The technician can then make a more informed decision about the upgrade needed.
An advantage of a configuration management application is that the entire collection of systems can be reviewed to make sure any changes made to one system do not adversely affect any of the other systems Configuration management is also used in software development, where it is called Unified Configuration Management (UCM). Using UCM, developers can keep track of the source code, documentation, problems, changes requested, and changes made.
Change management

In a computer system environment, change management refers to a systematic approach to keeping track of the details of the system (for example, what operating system release is running on each computer and which fixes have been applied).

NEW QUESTION: 237
Telnet and rlogin use which protocol?
A. UDP.
B. SNMP.
C. TCP.
D. IGP.
Answer: C (LEAVE A REPLY)
TCP allows for reliabilty in connections which would be required for terminal emulation.
The following answers are incorrect:
UDP. Is incorrect because with User Datagram Protocol (UDP) you don't have a reliable transmission, datagrams could arrive out of sequence.
SNMP. Is incorrect because it is a network management protocol, Simple Network Management Protocol (SNMP).
IGP. Is incorrect because Interior Gateway Protocol (IGP) is used interally on a network.

NEW QUESTION: 238
How would an IP spoofing attack be best classified?
A. Session hijacking attack
B. Passive attack
C. Fragmentation attack
D. Sniffing attack
Answer: A (LEAVE A REPLY)
IP spoofing is used to convince a system that it is communicating with a
known entity that gives an intruder access. IP spoofing attacks is a common session
hijacking attack.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3:
Telecommunications and Network Security (page 77).

NEW QUESTION: 239
What physical characteristic does a retinal scan biometric device measure?
A. The amount of light reaching the retina
B. The amount of light reflected by the retina
C. The pattern of light receptors at the back of the eye
D. The pattern of blood vessels at the back of the eye
Answer: D (LEAVE A REPLY)
Section: Access Control

Explanation/Reference:
The retina, a thin nerve (1/50th of an inch) on the back of the eye, is the part of the eye which senses light and transmits impulses through the optic nerve to the brain - the equivalent of film in a camera. Blood vessels used for biometric identification are located along the neural retina, the outermost of retina's four cell layers.
The following answers are incorrect:
The amount of light reaching the retina The amount of light reaching the retina is not used in the biometric scan of the retina.
The amount of light reflected by the retina The amount of light reflected by the retina is not used in the biometric scan of the retina.
The pattern of light receptors at the back of the eye This is a distractor The following reference(s) were/was used to create this question:
Reference: Retina Scan Technology.
ISC2 Official Guide to the CBK, 2007 (Page 161)

NEW QUESTION: 240
Proxies works by transferring a copy of each accepted data packet from one network to another, thereby masking the:
A. data's payload
B. data's details
C. data's owner
D. data's origin
Answer: (SHOW ANSWER)
Explanation/Reference:
The application firewall (proxy) relays the traffic from a trusted host running a specific application to an untrusted server. It will appear to the untrusted server as if the request originated from the proxy server.
"Data's payload" is incorrect. Only the origin is changed.
"Data's details" is incorrect. Only the origin is changed.
"Data's owner" is incorrect. Only the origin is changed.
References:
CBK, p. 467
AIO3, pp. 486 - 490

NEW QUESTION: 241
A proxy is considered a:
A. first generation firewall.
B. third generation firewall.
C. second generation firewall.
D. fourth generation firewall.
Answer: C (LEAVE A REPLY)

The proxy (application layer firewall, circuit level proxy, or application proxy) is a second generation firewall
"First generation firewall" incorrect. A packet filtering firewall is a first generation firewall. "Third generation firewall" is incorrect. Stateful Firewall are considered third generation firewalls "Fourth generation firewall" is incorrect. Dynamic packet filtering firewalls are fourth generation firewalls
References:
CBK, p. 464 AIO3, pp. 482 - 484
Neither CBK or AIO3 use the generation terminology for firewall types but you will encounter it frequently as a practicing security professional. See http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm for a general discussion of the different generations.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 242
Which of the following is not one of the three goals of Integrity addressed by the Clark-Wilson model?
A. Prevention of the modification of information by unauthorized users.
B. Prevention of the unauthorized or unintentional modification of information by authorized users.
C. Preservation of the internal and external consistency.
D. Prevention of the modification of information by authorized users.
Answer: (SHOW ANSWER)
Explanation/Reference:
There is no need to prevent modification from authorized users. They are authorized and allowed to make the changes. On top of this, it is also NOT one of the goal of Integrity within Clark-Wilson.
As it turns out, the Biba model addresses only the first of the three integrity goals which is Prevention of the modification of information by unauthorized users. Clark-Wilson addresses all three goals of integrity.
The Clark-Wilson model improves on Biba by focusing on integrity at the transaction level and addressing three major goals of integrity in a commercial environment. In addition to preventing changes by unauthorized subjects, Clark and Wilson realized that high-integrity systems would also have to prevent undesirable changes by authorized subjects and to ensure that the system continued to behave consistently. It also recognized that it would need to ensure that there is constant mediation between every subject and every object if such integrity was going to be maintained.
Integrity is addressed through the following three goals:
1. Prevention of the modification of information by unauthorized users.

2. Prevention of the unauthorized or unintentional modification of information by authorized users.
3. Preservation of the internal and external consistency.
The following reference(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17689-17694). Auerbach Publications. Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

NEW QUESTION: 243
How can an individual/person best be identified or authenticated to prevent local masquarading attacks?
A. UserId and password
B. Smart card and PIN code
C. Two-factor authentication
D. Biometrics
Answer: (SHOW ANSWER)
Explanation/Reference:
The only way to be truly positive in authenticating identity for access is to base the authentication on the physical attributes of the persons themselves (i.e., biometric identification). Physical attributes cannot be shared, borrowed, or duplicated. They ensure that you do identify the person, however they are not perfect and they would have to be supplemented by another factor.
Some people are getting thrown off by the term Masquarade. In general, a masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. Spoofing is another term used to describe this type of attack as well.
A UserId only provides for identification.
A password is a weak authentication mechanism since passwords can be disclosed, shared, written down, and more.
A smart card can be stolen and its corresponding PIN code can be guessed by an intruder. A smartcard can be borrowed by a friend of yours and you would have no clue as to who is really logging in using that smart card.
Any form of two-factor authentication not involving biometrics cannot be as reliable as a biometric system to identify the person.
Biometric identifying verification systems control people. If the person with the correct hand, eye, face, signature, or voice is not present, the identification and verification cannot take place and the desired action (i.e., portal passage, data, or resource access) does not occur.
As has been demonstrated many times, adversaries and criminals obtain and successfully use access cards, even those that require the addition of a PIN. This is because these systems control only pieces of plastic (and sometimes information), rather than people. Real asset and resource protection can only be

accomplished by people, not cards and information, because unauthorized persons can (and do) obtain the cards and information.
Further, life-cycle costs are significantly reduced because no card or PIN administration system or personnel are required. The authorized person does not lose physical characteristics (i.e., hands, face, eyes, signature, or voice), but cards and PINs are continuously lost, stolen, or forgotten. This is why card access systems require systems and people to administer, control, record, and issue (new) cards and PINs. Moreover, the cards are an expensive and recurring cost.
NOTE FROM CLEMENT:
This question has been generating lots of interest. The keyword in the question is: Individual (the person) and also the authenticated portion as well.
I totally agree with you that Two Factors or Strong Authentication would be the strongest means of authentication. However the question is not asking what is the strongest mean of authentication, it is asking what is the best way to identify the user (individual) behind the technology. When answering questions do not make assumptions to facts not presented in the question or answers.
Nothing can beat Biometrics in such case. You cannot lend your fingerprint and pin to someone else, you cannot borrow one of my eye balls to defeat the Iris or Retina scan. This is why it is the best method to authenticate the user.
I think the reference is playing with semantics and that makes it a bit confusing. I have improved the question to make it a lot clearer and I have also improve the explanations attached with the question.
The reference mentioned above refers to authenticating the identity for access. So the distinction is being made that there is identity and there is authentication. In the case of physical security the enrollment process is where the identity of the user would be validated and then the biometrics features provided by the user would authenticate the user on a one to one matching basis (for authentication) with the reference contained in the database of biometrics templates. In the case of system access, the user might have to provide a username, a pin, a passphrase, a smart card, and then provide his biometric attributes.
Biometric can also be used for Identification purpose where you do a one to many match. You take a facial scan of someone within an airport and you attempt to match it with a large database of known criminal and terrorists. This is how you could use biometric for Identification.
There are always THREE means of authentication, they are:
Something you know (Type 1)
Something you have (Type 2)
Something you are (Type 3)
Reference(s) used for this question:
TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1)
,2000, CRC Press, Chapter 1, Biometric Identification (page 7).
and
Search Security at http://searchsecurity.techtarget.com/definition/masquerade

NEW QUESTION: 244

Which of the following was designed as a more fault-tolerant topology than Ethernet, and very resilient when properly implemented?

A. Token Link.

B. Token system.

C. Token Ring.

D. Duplicate ring.

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Token Ring was designed to be a more fault-tolerant topology than Ethernet, and can be a very resilient topology when properly implemented.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.

NEW QUESTION: 245

What is the maximum number of different keys that can be used when encrypting with Triple DES?

A. 1

B. 2

C. 3

D. 4

Answer: C (LEAVE A REPLY)

Explanation/Reference:

Triple DES encrypts a message three times. This encryption can be accomplished in several ways. The most secure form of triple DES is when the three encryptions are performed with three different keys.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 152).

NEW QUESTION: 246

Which of the following can be defined as an Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client?

A. IMAP4

B. SMTP

C. MIME

D. PEM

Answer: A (LEAVE A REPLY)

RFC 2828 (Internet Security Glossary) defines the Internet Message Access Protocol, version 4 (IMAP4) as an Internet protocol by which a client workstation can dynamically access a mailbox on a server host to manipulate and retrieve mail messages that the server has received and is holding for the client. IMAP4 has mechanisms for optionally authenticating a client to a server and providing other security services.

MIME is the MultiPurpose Internet Mail Extension. MIME extends the format of Internet mail to allow non-US-ASCII textual messages, non-textual messages, multipart message bodies, and non-US-ASCII information in message headers.
Simple Mail Transfer Protocol (SMTP) is a TCP-based, application-layer, Internet Standard protocol for moving electronic mail messages from one computer to another.
Privacy Enhanced Mail (PEM) is an Internet protocol to provide data confidentiality, data integrity, and data origin authentication for electronic mail.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 247
When should a post-mortem review meeting be held after an intrusion has been properly taken care of?
A. Within the first three months after the investigation of the intrusion is completed.
B. Within the first week after prosecution of intruders have taken place, whether successful or not.
C. Within the first month after the investigation of the intrusion is completed.
D. Within the first week of completing the investigation of the intrusion.
Answer: (SHOW ANSWER)
Explanation/Reference:
A post-mortem review meeting should be held with all involved parties within three to five working days of completing the investigation of the intrusion. Otherwise, participants are likely to forget critical information. Even if it enabled an organization to validate the correctness of its chain of custody of evidence, it would not make sense to wait until prosecution is complete because it would take too much time and many cases of intrusion never get to court anyway.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (page 297).

NEW QUESTION: 248
What is the PRIMARY goal of incident handling?
A. Successfully retrieve all evidence that can be used to prosecute
B. Improve the company's ability to be prepared for threats and disasters
C. Improve the company's disaster recovery plan
D. Contain and repair any damage caused by an event.
Answer: (SHOW ANSWER)
This is the PRIMARY goal of an incident handling process.
The other answers are incorrect because :
Successfully retrieve all evidence that can be used to prosecute is more often used in identifying weaknesses than in prosecuting.
Improve the company's ability to be prepared for threats and disasters is more appropriate for a disaster recovery plan.
Improve the company's disaster recovery plan is also more appropriate for disaster recovery plan.
Reference : Shon Harris AIO v3 , Chapter - 10 : Law, Investigation, and Ethics , Page :

727-728

NEW QUESTION: 249
During the testing of the business continuity plan (BCP), which of the following methods of results analysis provides the BEST assurance that the plan is workable?
A. Measurement of accuracy
B. Elapsed time for completion of critical tasks
C. Quantitatively measuring the results of the test
D. Evaluation of the observed test results
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
It is important to have ways to measure the success of the plan and tests against the stated objectives. Therefore, results must be quantitatively gauged as opposed to an evaluation based only on observation. Quantitatively measuring the results of the test involves a generic statement measuring all the activities performed during BCP, which gives the best assurance of an effective plan. Although choices A and B are also quantitative, they relate to specific areas, or an analysis of results from one viewpoint, namely the accuracy of the results and the elapsed time.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 5: Disaster Recovery and Business Continuity (page 269).

NEW QUESTION: 250
Which of the following exemplifies proper separation of duties?
A. Operators are not permitted modify the system time.
B. Programmers are permitted to use the system console.
C. Console operators are permitted to mount tapes and disks.
D. Tape operators are permitted to use the system console.
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
This is an example of Separation of Duties because operators are prevented from modifying the system time which could lead to fraud. Tasks of this nature should be performed by they system administrators. AIO defines Separation of Duties as a security principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.
The following answers are incorrect:
Programmers are permitted to use the system console. Is incorrect because programmers should not be permitted to use the system console, this task should be performed by operators. Allowing programmers access to the system console could allow fraud to occur so this is not an example of Separation of Duties..
Console operators are permitted to mount tapes and disks. Is incorrect because operators should be able to mount tapes and disks so this is not an example of Separation of Duties.

Tape operators are permitted to use the system console. Is incorrect because operators should be able to use the system console so this is not an example of Separation of Duties.
References:
OIG CBK Access Control (page 98 - 101)
AIOv3 Access Control (page 182)

NEW QUESTION: 251
The concept of best effort delivery is best associated with?
A. TCP
B. HTTP
C. RSVP
D. IP
Answer: (SHOW ANSWER)
Explanation/Reference:
The Internet Protocol (IP) is a data-oriented protocol used for communicating data across a packet-switched internetwork. IP provides an unreliable service (i.e., best effort delivery). This means that the network makes no guarantees about the packet.
Low-level connectionless protocols such as DDP (under Appletalk) and IP usually provide best-effort delivery of data.
Best-effort delivery means that the protocol attempts to deliver any packets that meet certain requirements, such as containing a valid destination address, but the protocol does not inform the sender when it is unable to deliver the data, nor does it attempt to recover from error conditions and data loss.
Higher-level protocols such as TCP on the other hand, can provide reliable delivery of data. Reliable delivery includes error checking and recovery from error or loss of data.
HTTP is the HyperText Transport Protocol used to establish connections to a web server and thus one of the higher level protocol using TCP to ensure delivery of all bytes between the client and the server. It was not a good choice according to the question presented.
Here is another definition from the TCP/IP guide at: http://www.tcpipguide.com/free/t_IPOverviewandKeyOperationalCharacteristics.htm
Delivered Unreliably: IP is said to be an "unreliable protocol". That doesn't mean that one day your IP software will decide to go fishing rather than run your network. J It does mean that when datagrams are sent from device A to device B, device A just sends each one and then moves on to the next. IP doesn't keep track of the ones it sent. It does not provide reliability or service quality capabilities such as error protection for the data it sends (though it does on the IP header), flow control or retransmission of lost datagrams.
For this reason, IP is sometimes called a best-effort protocol. It does what it can to get data to where it needs to go, but "makes no guarantees" that the data will actually get there.

NEW QUESTION: 252
The major objective of system configuration management is which of the following?
A. system maintenance.

B. system stability.
C. system operations.
D. system tracking.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
A major objective with Configuration Management is stability. The changes to the system are controlled so that they don't lead to weaknesses or faults in th system.
The following answers are incorrect:
system maintenance. Is incorrect because it is not the best answer. Configuration Management does control the changes to the system but it is not as important as the overall stability of the system.
system operations. Is incorrect because it is not the best answer, the overall stability of the system is much more important.
system tracking. Is incorrect because while tracking changes is important, it is not the best answer. The overall stability of the system is much more important.

NEW QUESTION: 253
An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):
A. active attack
B. outside attack
C. inside attack
D. passive attack
Answer: (SHOW ANSWER)
Explanation/Reference:
An inside attack is an attack initiated by an entity inside the security perimeter, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization whereas an outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system. An active attack attempts to alter system resources to affect their operation and a passive attack attempts to learn or make use of the information from the system but does not affect system resources.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 254
Which of the following DoS attacks use ICMP? (Choose two)
A. SYN attack
B. Smurf attack
C. Ping of death
D. UDP flood
E. NMAP
Answer: (SHOW ANSWER)

The ping-of-death attack sends an ICMP packet so large that some systems crash before they can process all of the information. The Smurf attack also manipulates ICMP. The other answers are incorrect. NMAP is a port scanning and banner grabbing tool.

NEW QUESTION: 255
Which element must computer evidence have to be admissible in court?
A. It must be relevant.
B. It must be annotated.
C. It must be printed.
D. It must contain source code.
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 256
Why is infrared generally considered to be more secure to eavesdropping than multidirectional radio transmissions?
A. Because infrared eavesdropping requires more sophisticated equipment.
B. Because infrared operates only over short distances.
C. Because infrared requires direct line-of-sight paths.
D. Because infrared operates at extra-low frequencies (ELF).
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Infrared is generally considered to be more secure to eavesdropping than multidirectional radio transmissions because infrared requires direct line-of-sight paths.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 173).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 257
What is the role of IKE within the IPsec protocol?

A. peer authentication and key exchange
B. data encryption
C. data signature
D. enforcing quality of service
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Reference: RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand & HARKINS, Dan, Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

NEW QUESTION: 258
Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer 7 of the ISO/OSI Model?
A. Bridge
B. Repeater
C. Router
D. Gateway
Answer: D (LEAVE A REPLY)
A gateway is used to connect two networks using dissimilar protocols at the lower layers or it could also be at the highest level of the protocol stack.
Important Note:
For the purpose of the exam, you have to remember that a gateway is not synonymous to the term firewall.
The second thing you must remembers is the fact that a gateway act as a translation device.
It could be used to translate from IPX to TCP/IP for example. It could be used to convert different types of applications protocols and allow them to communicate together. A gateway could be at any of the OSI layers but usually tend to be higher up in the stack.
For your exam you should know the information below:
Repeaters
A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel. Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal. A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to

another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.
Repeater
Image Reference- http://www.erg.abdn.ac.uk/~gorry/course/images/repeater.gif
Bridges A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.
Bridge C:\Users\MCS\Desktop\1.jpg
Image Reference- http://www.oreillynet.com/network/2001/01/30/graphics/bridge.jpg
Routers Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.
Router and Switch
Image Reference- http://www.computer-networking-success.com/images/router-switch.jpg
Switches Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.
Gateways Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.
Gateway Server C:\Users\MCS\Desktop\1.jpg
Image
Referencehttp://static.howtoforge.com/images/screenshots/556af08d5e43aa768260f9e589dc547f3024.jpg
The following answers are incorrect:
Repeater - A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.
Bridges - A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is

on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.
Routers - Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary.
Following reference(s) were/was used to create this question: CISA review manual 2014 Page number 263 Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 and 230

NEW QUESTION: 259
What does the simple security (ss) property mean in the Bell-LaPadula model?
A. No read up
B. No write down
C. No read down
D. No write up
Answer: (SHOW ANSWER)
Explanation/Reference:
The ss (simple security) property of the Bell-LaPadula access control model states that reading of information by a subject at a lower sensitivity level from an object at a higher sensitivity level is not permitted (no read up).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 202).

NEW QUESTION: 260
What security model is dependent on security labels?
A. Discretionary access control
B. Label-based access control
C. Mandatory access control
D. Non-discretionary access control
Answer: (SHOW ANSWER)
Explanation/Reference:
With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and the classification or sensitivity of the object.
Label- based access control is not defined.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION: 261
In the course of responding to and handling an incident, you work on determining the root cause of the incident.

In which step are you in?
A. Recovery
B. Containment
C. Triage
D. Analysis and tracking
Answer: D (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
In this step, your main objective is to examine and analyze what has occurred and focus on determining the root cause of the incident.
Recovery is incorrect as recovery is about resuming operations or bringing affected systems back into production Containment is incorrect as containment is about reducing the potential impact of an incident.
Triage is incorrect as triage is about determining the seriousness of the incident and filtering out false positives Reference:
Official Guide to the CISSP CBK, pages 700-704

NEW QUESTION: 262
What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?
A. Central station alarm
B. Proprietary alarm
C. A remote station alarm
D. An auxiliary station alarm
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Auxiliary station alarms automatically cause an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters. They are usually Municipal Fire Alarm Boxes are installed at your business or building, they are wired directly into the fire station.
Central station alarms are operated by private security organizations. It is very similar to a proprietary alarm system (see below). However, the biggest difference is the monitoring and receiving of alarm is done off site at a central location manned by non staff members. It is a third party.
Proprietary alarms are similar to central stations alarms except that monitoring is performed directly on the protected property. This type of alarm is usually use to protect large industrials or commercial buildings.
Each of the buildings in the same vincinity has their own alarm system, they are all wired together at a central location within one of the building acting as a common receiving point. This point is usually far away from the other building so it is not under the same danger. It is usually man 24 hours a day by a trained team who knows how to react under different conditions.

A remote station alarm is a direct connection between the signal-initiating device at the protected property and the signal-receiving device located at a remote station, such as the fire station or usually a monitoring service. This is the most popular type of implementation and the owner of the premise must pay a monthly monitoring fee. This is what most people use in their home where they get a company like ADT to receive the alarms on their behalf.
A remote system differs from an auxiliary system in that it does not use the municipal fire of police alarm circuits.
Reference(s) used for this question:
ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 11: Physical Security (page 211).
and
Great presentation J.T.A. Stone on SlideShare

NEW QUESTION: 263
The fact that a network-based IDS reviews packets payload and headers enable which of the following?
A. Detection of denial of service
B. Detection of all viruses
C. Detection of data corruption
D. Detection of all password guessing attacks
Answer: (SHOW ANSWER)
Explanation/Reference:
Because a network-based IDS reviews packets and headers, denial of service attacks can also be detected.
This question is an easy question if you go through the process of elimination. When you see an answer containing the keyword: ALL It is something a give away that it is not the proper answer. On the real exam you may encounter a few question where the use of the work ALL renders the choice invalid. Pay close attention to such keyword.
The following are incorrect answers:
Even though most IDSs can detect some viruses and some password guessing attacks, they cannot detect ALL viruses or ALL password guessing attacks. Therefore these two answers are only detractors.
Unless the IDS knows the valid values for a certain dataset, it can NOT detect data corruption.
Reference used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

NEW QUESTION: 264
What is called an exception to the search warrant requirement that allows an officer to conduct a search without having the warrant in-hand if probable cause is present and destruction of the evidence is deemed imminent?
A. Evidence Circumstance Doctrine
B. Exigent Circumstance Doctrine
C. Evidence of Admissibility Doctrine

D. Exigent Probable Doctrine

Answer: B (LEAVE A REPLY)

Explanation/Reference:

An Exigent Circumstance is an unusual and time-sensitive circumstance that justifies conduct that might not be permissible or lawful in other circumstances.

For example, exigent circumstances may justify actions by law enforcement officers acting without a warrant such as a mortal danger to a young child. Examples of other exigent circumstances include protecting evidence or property from imminent destruction.

In US v Martinez, Justice Thomas of the United States Court of Appeal used these words:

"As a general rule, we define exigent circumstances as those circumstances that would cause a reasonable person to believe that entry was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."

In Alvarado, Justice Blackburn of the Court of Appeals of Georgia referred to exigent circumstances in the context of a drug bust:

"The exigent circumstance doctrine provides that when probable cause has been established to believe that evidence will be removed or destroyed before a warrant can be obtained, a warrantless search and seizure can be justified. As many courts have noted, the need for the exigent circumstance doctrine is particularly compelling in narcotics cases, because contraband and records can be easily and quickly destroyed while a search is progressing. Police officers relying on this exception must demonstrate an objectively reasonable basis for deciding that immediate action is required." All of the other answers were only detractors made up and not legal terms.

Reference(s) used for this question:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 313.

and

http://www.duhaime.org/LegalDictionary/E/ExigentCircumstances.aspx

NEW QUESTION: 265

Why does fiber optic communication technology have significant security advantage over other transmission technology?

A. Higher data rates can be transmitted.

B. Interception of data traffic is more difficult.

C. Traffic analysis is prevented by multiplexing.

D. Single and double-bit errors are correctable.

Answer: B (LEAVE A REPLY)

Explanation/Reference:

It would be correct to select the first answer if the world "security" was not in the question.

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 266

Which of the following is an advantage of a qualitative over a quantitative risk analysis?
A. It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
B. It provides specific quantifiable measurements of the magnitude of the impacts.
C. It makes a cost-benefit analysis of recommended controls easier.
D. It can easily be automated.
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. It does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-analysis of any recommended controls difficult. Since it involves a consensus of export and some guesswork based on the experience of Subject Matter Experts (SME's), it can not be easily automated.
Reference used for this question:
STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 23).

NEW QUESTION: 267
Which element must computer evidence have to be admissible in court?
A. It must be relevant.
B. It must be annotated.
C. It must be printed.
D. It must contain source code.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 268
Which of the following is an example of a connectionless communication protocol?
A. UDP
B. X.25
C. Packet switching
D. TCP
Answer: A (LEAVE A REPLY)
UDP is an example of connectionless communication protocol, wherein no connection needs to be established before data can be exchanged.
In telecommunications, connectionless describes communication between two network end points in which a message can be sent from one end point to another without prior arrangement. The device at one end of the communication transmits data addressed to the other, without first ensuring that the recipient is available and ready to receive the data. Some protocols allow for error correction by

requested retransmission. Internet Protocol (IP) and User Datagram Protocol (UDP) are connectionless protocols.
Connectionless protocols are also described as stateless because the endpoints have no protocol-defined way to remember where they are in a "conversation" of message exchanges. List of connectionless protocols
Hypertext Transfer Protocol IP UDP ICMP IPX TIPC NetBEUI
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 86). and https://secure.wikimedia.org/wikipedia/en/wiki/Connectionless_protocol

NEW QUESTION: 269
What can be defined as a table of subjects and objects indicating what actions individual subjects can take upon individual objects?
A. A capacity table
B. An access control list
C. An access control matrix
D. A capability table
Answer: C (LEAVE A REPLY)
The matrix lists the users, groups and roles down the left side and the
resources and functions across the top. The cells of the matrix can either indicate that
access is allowed or indicate the type of access. CBK pp 317 - 318.
AIO3, p. 169 describes it as a table if subjects and objects specifying the access rights a
certain subject possesses pertaining to specific objects.
In either case, the matrix is a way of analyzing the access control needed by a population
of subjects to a population of objects. This access control can be applied using rules,
ACL's, capability tables, etc.
"A capacity table" is incorrect.
This answer is a trap for the unwary -- it sounds a little like "capability table" but is just there
to distract you.
"An access control list" is incorrect.
"It [ACL] specifies a list of users [subjects] who are allowed access to each object" CBK, p. 188 Access control lists (ACL) could be used to implement the rules identified by an access control matrix but is different from the matrix itself.
"A capability table" is incorrect.
"Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's posession of a capability (or ticket) for the object." CBK, pp. 191-192. To put it another way, as noted in AIO3 on p. 169, "A capabiltiy table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL."

Again, a capability table could be used to implement the rules identified by an access control matrix but is different from the matrix itself.
References:
CBK pp. 191-192, 317-318 AIO3, p. 169

NEW QUESTION: 270
Which of the following models does NOT include data integrity or conflict of interest?
A. Biba
B. Clark-Wilson
C. Bell-LaPadula
D. Brewer-Nash
Answer: C (LEAVE A REPLY)
Bell LaPadula model (Bell 1975): The granularity of objects and subjects is not predefined, but the model prescribes simple access rights. Based on simple access restrictions the Bell LaPadula model enforces a discretionary access control policy enhanced with mandatory rules. Applications with rigid confidentiality requirements and without strong integrity requirements may properly be modeled.
These simple rights combined with the mandatory rules of the policy considerably restrict
the spectrum of applications which can be appropriately modeled.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
Also check:
Proceedings of the IFIP TC11 12th International Conference on Information Security,
Samos (Greece), May 1996, On Security Models.

NEW QUESTION: 271
Which of the following statements pertaining to disk mirroring is incorrect?
A. Mirroring offers better performance in read operations but writing hinders system performance.
B. Mirroring is a hardware-based solution only.
C. Mirroring offers a higher fault tolerance than parity.
D. Mirroring is usually the less cost-effective solution.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
With mirroring, the system writes the data simultaneously to separate drives or arrays.
The advantage of mirroring are minimal downtime, simple data recovery, and increased performance in reading from the disk.
The disadvantage of mirroring is that both drives or disk arrays are processing in the writing to disks function, which can hinder system performance.
Mirroring has a high fault tolerance and can be implemented either through a hardware RAID controller or through the operating system. Since it requires twice the disk space than actual data, mirroring is the less cost- efficient data redundancy strategy.

Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page
45).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 272
Risk can be totally eliminated through planning, control, procedures, and insurance.
(True / False)
A. True
B. False
Answer: B (LEAVE A REPLY)
Whereas risk can be reduced to an acceptable level, it can NEVER be totally eliminated.

NEW QUESTION: 273
Access Control techniques do not include which of the following?
A. Rule-Based Access Controls
B. Role-Based Access Control
C. Mandatory Access Control
D. Random Number Based Access Control
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Access Control Techniques
Discretionary Access Control
Mandatory Access Control
Lattice Based Access Control
Rule-Based Access Control
Role-Based Access Control
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

NEW QUESTION: 274
In the statement below, fill in the blank:

Law enforcement agencies must get a warrant to search and seize an individual's property, as stated in the _____ Amendment.

A. First.

B. Second.

C. Third.

D. Fourth.

Answer: D (LEAVE A REPLY)

The Fourth Amendment does not apply to a seizure or an arrest by private citizens.

Search and seizure activities can get tricky depending on what is being searched for and where.

For example, American citizens are protected by the Fourth Amendment against unlawful search and seizure, so law enforcement agencies must have probable cause and request a search warrant from a judge or court before conducting such a search.

The actual search can only take place in the areas outlined by the warrant. The Fourth Amendment does not apply to actions by private citizens unless they are acting as police agents. So, for example, if Kristy's boss warned all employees that the management could remove files from their computers at any time, and her boss was not a police officer or acting as a police agent, she could not successfully claim that her Fourth Amendment rights were violated. Kristy's boss may have violated some specific privacy laws, but he did not violate Kristy's Fourth Amendment rights.

In some circumstances, a law enforcement agent may seize evidence that is not included in the warrant, such as if the suspect tries to destroy the evidence. In other words, if there is an impending possibility that evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction. This is referred to as exigent circumstances, and a judge will later decide whether the seizure was proper and legal before allowing the evidence to be admitted. For example, if a police officer had a search warrant that allowed him to search a suspect's living room but no other rooms, and then he saw the suspect dumping cocaine down the toilet, the police officer could seize the cocaine even though it was in a room not covered under his search warrant. After evidence is gathered, the chain of custody needs to be enacted and enforced to make sure the evidence's integrity is not compromised.

All other choices were only detractors.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1057). McGraw-Hill. Kindle Edition.

NEW QUESTION: 275

The IP header contains a protocol field. If this field contains the value of 51, what type of data is contained within the ip datagram?

A. Transmission Control Protocol (TCP)

B. Authentication Header (AH)
C. User datagram protocol (UDP)
D. Internet Control Message Protocol (ICMP)
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
TCP has the value of 6
UDP has the value of 17
ICMP has the value of 1
Reference:
SANS http://www.sans.org/resources/tcpip.pdf?ref=3871

NEW QUESTION: 276
One of the following assertions is NOT a characteristic of Internet Protocol Security (IPsec)
A. Data cannot be read by unauthorized parties
B. The identity of all IPsec endpoints are confirmed by other endpoints
C. Data is delivered in the exact order in which it is sent
D. The number of packets being exchanged can be counted.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
IPSec provide replay protection that ensures data is not delivered multiple times, however IPsec does not ensure that data is delivered in the exact order in which it is sent. IPSEC uses TCP and packets may be delivered out of order to the receiving side depending which route was taken by the packet.
Internet Protocol Security (IPsec) has emerged as the most commonly used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over IP networks. Depending on how IPsec is implemented and configured, it can provide any combination of the following types of protection:
Confidentiality. IPsec can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.
Integrity. IPsec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.
Peer Authentication. Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.
Replay Protection. The same data is not delivered multiple times, and data is not delivered grossly out of order. However, IPsec does not ensure that data is delivered in the exact order in which it is sent.
Traffic Analysis Protection. A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged. However, the number of packets being exchanged can be counted.

Access Control. IPsec endpoints can perform filtering to ensure that only authorized IPsec users can access particular network resources. IPsec endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing.
The following are incorrect answers because they are all features provided by IPSEC:
"Data cannot be read by unauthorized parties" is wrong because IPsec provides confidentiality through the usage of the Encapsulating Security Protocol (ESP), once encrypted the data cannot be read by unauthorized parties because they have access only to the ciphertext. This is accomplished by encrypting data using a cryptographic algorithm and a session key, a value known only to the two parties exchanging data. The data can only be decrypted by someone who has a copy of the session key.
"The identity of all IPsec endpoints are confirmed by other endpoints" is wrong because IPsec provides peer authentication: Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.
"The number of packets being exchanged can be counted" is wrong because although IPsec provides traffic protection where a person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged, the number of packets being exchanged still can be counted.
Reference(s) used for this question:
NIST 800-77 Guide to IPsec VPNs . Pages 2-3 to 2-4

NEW QUESTION: 277
Each of the following is a valid step in handling incidents except _____
A. Prosecute
B. Recover
C. Review
D. Contain
E. Identify
F. Prepare
Answer: A (LEAVE A REPLY)

NEW QUESTION: 278
SMTP can best be described as:
A. a host-to-host email protocol.
B. an email retrieval protocol.
C. a web-based e-mail reading protocol.
D. a standard defining the format of e-mail messages.
Answer: (SHOW ANSWER)
Simple Mail Transfer Protocol (SMTP) is a host-to-host email protocol. An SMTP server accepts email messages from other systems and stores them for the addressees. Stored email can be read in various ways. Users with interactive accounts on the email server machine can read the email using local email applications. Users on other systems can download their email via email clients using POP or IMAP email

retrieval protocols. Sometimes mail can also be read through a web-based interface (using HTTP or HTTPS). MIME is a standard defining the format of e-mail messages, as stated in RFC2045.
Source: GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (pages 91-92).

NEW QUESTION: 279
Which OSI/ISO layer does a SOCKS server operate at?
A. Session layer
B. Transport layer
C. Network layer
D. Data link layer
Answer: A (LEAVE A REPLY)
A SOCKS based server operates at the Session layer of the OSI model.
SOCKS is an Internet protocol that allows client-server applications to transparently use the services of a network firewall. SOCKS is an abbreviation for "SOCKetS". As of Version 5 of SOCK, both UDP and TCP is supported.
One of the best known circuit-level proxies is SOCKS proxy server. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server, without requiring direct "IP-reachability"
The protocol was originally developed by David Koblas, a system administrator of MIPS Computer Systems. After MIPS was taken over by Silicon Graphics in 1992, Koblas presented a paper on SOCKS at that year's Usenix Security Symposium and SOCKS became publicly available. The protocol was extended to version 4 by Ying-Da Lee of NEC.
SOCKS includes two components, the SOCKS server and the SOCKS client.
The SOCKS protocol performs four functions:
Making connection requests Setting up proxy circuits Relaying application data Performing user authentication (optional)
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 96). and http://en.wikipedia.org/wiki/SOCKS and http://www.faqs.org/rfcs/rfc1928.html and The ISC2 OIG on page 619

NEW QUESTION: 280
Which security model ensures that actions that take place at a higher security level do not affect actions that take place at a lower level?
A. The Bell-LaPadula model
B. The information flow model
C. The noninterference model
D. The Clark-Wilson model
Answer: C (LEAVE A REPLY)
The goal of a noninterference model is to strictly separate differing security

levels to assure that higher-level actions do not determine what lower-level users can see.
This is in contrast to other security models that control information flows between differing levels of users, By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.
The model ensures that any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level.
It is not concerned with the flow of data, but rather with what a subject knows about the state of the system. So if an entity at a higher security level performs an action, it can not change the state for the entity at the lower level.
The model also addresses the inference attack that occurs when some one has access to some type of information and can infer(guess) something that he does not have the clearance level or authority to know.
The following are incorrect answers:
The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned only with confidentiality and bases access control decisions on the classfication of objects and the clearences of subjects.
The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security classes. Information will be allowed to flow only in accordance with the security policy.
The Clark-Wilson model is incorrect. The Clark-Wilson model is concerned with change control and assuring that all modifications to objects preserve integrity by means of well-formed transactions and usage of an access triple (subjet - interface - object).
References:
CBK, pp 325 - 326 AIO3, pp. 290 - 291 AIOv4 Security Architecture and Design (page 345) AIOv5 Security Architecture and Design (pages 347 - 348)
https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Models#Noninterference_Models

NEW QUESTION: 281
What is the most correct choice below when talking about the steps to resume normal operation at the primary site after the green light has been given by the salvage team?
A. The most critical operations are moved from alternate site to primary site before others
B. Operation may be carried by a completely different team than disaster recovery team
C. The least critical functions should be moved back first
D. You moves items back in the same order as the categories document in your plan or exactly in the same order as you did on your way to the alternate site
Answer: (SHOW ANSWER)
It's interesting to note that the steps to resume normal processing operations will be different than the steps of the recovery plan; that is, the least critical work should be brought back first to the primary site. The most important point above in the steps would be to move the least critical items or resources back to the primary site first. This way you can ensure that the site was really
well prepared and that all is working fine.

Before that first step would be done, you would get the green light from the salvage team that it is fine to move back to the primary site. The first step after getting the green light would be to move the least critical elements first.
As stated in the Shon Harris book:
The least critical functions should be moved back first, so if there are issues in network configurations or connectivity, or important steps were not carried out, the critical operations of the company are not negatively affected. Why go through the trouble of moving the most critical systems and operations to a safe and stable site, only to return it to a main site that is untested? Let the less critical departments act as the canary. If they survive, then move over the more critical components of the company.
When it is time for the company to move back into its original site or a new site, the company enters the reconstitution phase. A company is not out of an emergency state until it is back in operation at the original primary site or a new site that was constructed to replace the primary site, because the company is always vulnerable while operating in a backup facility.
Many logistical issues need to be considered as to when a company must return from the alternate site to the original site. The following lists a few of these issues:
Ensuring the safety of employees
Ensuring an adequate environment is provided (power, facility infrastructure, water, HVAC)
Ensuring that the necessary equipment and supplies are present and in working order
Ensuring proper communications and connectivity methods are working
Properly testing the new environment
Once the coordinator, management, and salvage team sign off on the readiness of the facility, the salvage team should carry out the following steps:
Back up data from the alternate site and restore it within the new facility.
Carefully terminate contingency operations.
Securely transport equipment and personnel to the new facility.
All other choices are not the correct answer.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Location 19389). McGraw-Hill. Kindle Edition. and KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 290.

NEW QUESTION: 282
Single Sign-on (SSO) is characterized by which of the following advantages?
A. Convenience
B. Convenience and centralized administration
C. Convenience and centralized data administration
D. Convenience and centralized network administration
Answer: (SHOW ANSWER)

Convenience -Using single sign-on users have to type their passwords only once when they first log in to access all the network resources; and Centralized Administration as some single sign-on systems are built around a unified server administration system. This allows a single administrator to add and delete accounts across the entire network from one user interface.
The following answers are incorrect:
Convenience - alone this is not the correct answer.
Centralized Data or Network Administration - these are thrown in to mislead the student. Neither are a benefit to SSO, as these specifically should not be allowed with just an SSO.
References: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, page 35. TIPTON, Harold F. & HENRY, Kevin, Official (ISC)2 Guide to the CISSP CBK, 2007, page
180.

NEW QUESTION: 283
Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is not a component that achieves this type of security?
A. Administrative control mechanisms
B. Integrity control mechanisms
C. Technical control mechanisms
D. Physical control mechanisms
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Integrity Controls Mechanisms are not part of physical security. All of the other detractors were correct this one was the wrong one that does not belong to Physical Security. Below you have more details extracted from the SearchSecurity web site:
Information security depends on the security and management of the physical space in which computer systems operate. Domain 9 of the CISSP exam's Common Body of Knowledge addresses the challenges of securing the physical space, its systems and the people who work within it by use of administrative, technical and physical controls. The following Qs are covered:
Facilities management: The administrative processes that govern the maintenance and protection of the physical operations space, from site selection through emergency response.
Risks, issues and protection strategies: Risk identification and the selection of security protection components.
Perimeter security: Typical physical protection controls.
Facilities management
Facilities management is a complex component of corporate security that ranges from the planning of a secure physical site to the management of the physical information system environment. Facilities management responsibilities include site selection and physical security planning (i.e. facility construction, design and layout, fire and water damage protection, antitheft mechanisms, intrusion detection and security procedures.) Protections must extend to both people and assets. The necessary

level of protection depends on the value of the assets and data. CISSP® candidates must learn the concept of critical-path analysis as a means of determining a component's business function criticality relative to the cost of operation and replacement. Furthermore, students need to gain an understanding of the optimal location and physical attributes of a secure facility. Among the Qs covered in this domain are site inspection, location, accessibility and obscurity, considering the area crime rate, and the likelihood of natural hazards such as floods or earthquakes.

This domain also covers the quality of construction material, such as its protective qualities and load capabilities, as well as how to lay out the structure to minimize risk of forcible entry and accidental damage. Regulatory compliance is also touched on, as is preferred proximity to civil protection services, such as fire and police stations. Attention is given to computer and equipment rooms, including their location, configuration (entrance/egress requirements) and their proximity to wiring distribution centers at the site.

Physical risks, issues and protection strategies

An overview of physical security risks includes risk of theft, service interruption, physical damage, compromised system integrity and unauthorized disclosure of information. Interruptions to business can manifest due to loss of power, services, telecommunications connectivity and water supply. These can also seriously compromise electronic security monitoring alarm/response devices. Backup options are also covered in this domain, as is a strategy for quantifying the risk exposure by simple formula.

Investment in preventive security can be costly. Appropriate redundancy of people skills, systems and infrastructure must be based on the criticality of the data and assets to be preserved. Therefore a strategy is presented that helps determine the selection of cost appropriate controls. Among the Qs covered in this domain are regulatory and legal requirements, common standard security protections such as locks and fences, and the importance of establishing service level agreements for maintenance and disaster support.

Rounding out the optimization approach are simple calculations for determining mean time between failure and mean time to repair (used to estimate average equipment life expectancy) - essential for estimating the cost/benefit of purchasing and maintaining redundant equipment.

As the lifeblood of computer systems, special attention is placed on adequacy, quality and protection of power supplies. CISSP candidates need to understand power supply concepts and terminology, including those for quality (i.e. transient noise vs. clean power); types of interference (EMI and RFI); and types of interruptions such as power excess by spikes and surges, power loss by fault or blackout, and power degradation from sags and brownouts. A simple formula is presented for determining the total cost per hour for backup power. Proving power reliability through testing is recommended and the advantages of three power protection approaches are discussed (standby UPS, power line conditioners and backup sources) including minimum requirements for primary and alternate power provided.

Environmental controls are explored in this domain, including the value of positive pressure water drains and climate monitoring devices used to control temperature, humidity and reduce static electricity. Optimal temperatures and humidity settings are provided. Recommendations include strict procedures during emergencies, preventing typical risks (such as blocked fans), and the use of antistatic armbands and hygrometers. Positive pressurization for proper ventilation and monitoring for air born contaminants is stressed.

The pros and cons of several detection response systems are deeply explored in this domain. The concept of combustion, the classes of fire and fire extinguisher ratings are detailed. Mechanisms behind smoke- activated, heat-activated and flame-activated devices and Automatic Dial-up alarms are covered, along with their advantages, costs and shortcomings. Types of fire sources are distinguished and the effectiveness of fire suppression methods for each is included. For instance, Halon and its approved replacements are covered, as are the advantages and the inherent risks to equipment of the use of water sprinklers.

Administrative controls

The physical security domain also deals with administrative controls applied to physical sites and assets. The need for skilled personnel, knowledge sharing between them, separation of duties, and appropriate oversight in the care and maintenance of equipment and environments is stressed. A list of management duties including hiring checks, employee maintenance activities and recommended termination procedures is offered. Emergency measures include accountability for evacuation and system shutdown procedures, integration with disaster and business continuity plans, assuring documented procedures are easily available during different types of emergencies, the scheduling of periodic equipment testing, administrative reviews of documentation, procedures and recovery plans, responsibilities delegation, and personnel training and drills.

Perimeter security

Domain nine also covers the devices and techniques used to control access to a space. These include access control devices, surveillance monitoring, intrusion detection and corrective actions. Specifications are provided for optimal external boundary protection, including fence heights and placement, and lighting placement and types. Selection of door types and lock characteristics are covered. Surveillance methods and intrusion-detection methods are explained, including the use of video monitoring, guards, dogs, proximity detection systems, photoelectric/photometric systems, wave pattern devices, passive infrared systems, and sound and motion detectors, and current flow sensitivity devices that specifically address computer theft. Room lock types - both preset and cipher locks (and their variations) -- device locks, such as portable laptop locks, lockable server bays, switch control locks and slot locks, port controls, peripheral switch controls and cable trap locks are also covered. Personal access control methods used to identify authorized users for site entry are covered at length, noting social engineering risks such as piggybacking.

Wireless proximity devices, both user access and system sensing readers are covered (i.e. transponder based, passive devices and field powered devices) in this domain.

Now that you've been introduced to the key concepts of Domain 9, watch the Domain 9, Physical Security video

Return to the CISSP Essentials Security School main page

See all SearchSecurity.com's resources on CISSP certification training

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 280.

NEW QUESTION: 284

Related to information security, integrity is the opposite of which of the following?

A. abstraction
B. alteration
C. accreditation
D. application
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Integrity is the opposite of "alteration."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 285
A momentary high voltage is a:
A. spike
B. blackout
C. surge
D. fault
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Too much voltage for a short period of time is a spike.
Too much voltage for a long period of time is a surge.
Not enough voltage for a short period of time is a sag or dip
Not enough voltage for a long period of time is brownout
A short power interruption is a fault
A long power interruption is a blackout
You MUST know all of the power issues above for the purpose of the exam.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

NEW QUESTION: 286
What can be defined as an abstract machine that mediates all access to objects by subjects to ensure that subjects have the necessary access rights and to protect objects from unauthorized access?
A. The Reference Monitor
B. The Security Kernel
C. The Trusted Computing Base
D. The Security Domain
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The reference monitor refers to abstract machine that mediates all access to objects by subjects.

This question is asking for the concept that governs access by subjects to objects, thus the reference monitor is the best answer. While the security kernel is similar in nature, it is what actually enforces the concepts outlined in the reference monitor.

In operating systems architecture a reference monitor concept defines a set of design requirements on a reference validation mechanism, which enforces an access control policy over subjects' (e.g., processes and users) ability to perform operations (e.g., read and write) on objects (e.g., files and sockets) on a system. The properties of a reference monitor are:

The reference validation mechanism must always be invoked (complete mediation). Without this property, it is possible for an attacker to bypass the mechanism and violate the security policy.

The reference validation mechanism must be tamperproof (tamperproof). Without this property, an attacker can undermine the mechanism itself so that the security policy is not correctly enforced.

The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured (verifiable). Without this property, the mechanism might be flawed in such a way that the policy is not enforced.

For example, Windows 3.x and 9x operating systems were not built with a reference monitor, whereas the Windows NT line, which also includes Windows 2000 and Windows XP, was designed to contain a reference monitor, although it is not clear that its properties (tamperproof, etc.) have ever been independently verified, or what level of computer security it was intended to provide.

The claim is that a reference validation mechanism that satisfies the reference monitor concept will correctly enforce a system's access control policy, as it must be invoked to mediate all security-sensitive operations, must not be tampered, and has undergone complete analysis and testing to verify correctness. The abstract model of a reference monitor has been widely applied to any type of system that needs to enforce access control, and is considered to express the necessary and sufficient properties for any system making this security claim.

According to Ross Anderson, the reference monitor concept was introduced by James Anderson in an influential 1972 paper.

Systems evaluated at B3 and above by the Trusted Computer System Evaluation Criteria (TCSEC) must enforce the reference monitor concept.

The reference monitor, as defined in AIO V5 (Harris) is: "an access control concept that refers to an abstract machine that mediates all access to objects by subjects." The security kernel, as defined in AIO V5 (Harris) is: "the hardware, firmware, and software elements of a trusted computing based (TCB) that implement the reference monitor concept. The kernel must mediate all access between subjects and objects, be protected from modification, and be verifiable as correct." The trusted computing based (TCB), as defined in AIO V5 (Harris) is: "all of the protection mechanisms within a computer system (software, hardware, and firmware) that are responsible for enforcing a security policy." The security domain, "builds upon the definition of domain (a set of resources available to a subject) by adding the fact that resources withing this logical structure (domain) are working under the same security policy and managed by the same group." The following answers are incorrect:

"The security kernel" is incorrect. One of the places a reference monitor could be implemented is in the security kernel but this is not the best answer.

"The trusted computing base" is incorrect. The reference monitor is an important concept in the TCB but this is not the best answer.
"The security domain is incorrect." The reference monitor is an important concept in the security domain but this is not the best answer.
Reference(s) used for this question:
Official ISC2 Guide to the CBK, page 324
AIO Version 3, pp. 272 - 274
AIOv4 Security Architecture and Design (pages 327 - 328)
AIOv5 Security Architecture and Design (pages 330 - 331)
Wikipedia article at https://en.wikipedia.org/wiki/Reference_monitor

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 287
Which of the following are REGISTERED PORTS as defined by IANA ?
A. Ports 128 to 255
B. Ports 1024 to 49151
C. Ports 1025 to 65535
D. Ports 1024 to 32767
Answer: B (LEAVE A REPLY)
Ports 1024 to 49151 has been defined as REGISTERED PORTS by IANA.
A registered port is a network port (a sub-address defined within the Internet Protocol, in the range 1-65535) assigned by the Internet Assigned Numbers Authority (IANA) (or by Internet Corporation for Assigned Names and Numbers (ICANN) before March 21, 2001) for use with a certain protocol or application.
Ports with numbers lower than those of the registered ports are called well known ports; ports with numbers greater than those of the registered ports are called dynamic and/or private ports.
Ports 0-1023 - well known ports Ports 1024-49151 - Registered port: vendors use for applications Ports >49151 - dynamic / private ports
The other answers are not correct
Reference(s) used for this question: http://en.wikipedia.org/wiki/Registered_port

NEW QUESTION: 288

Organizations should consider which of the following first before allowing external access to their LANs via the Internet?
A. plan for implementing workstation locking mechanisms.
B. plan for protecting the modem pool.
C. plan for providing the user with his account usage information.
D. plan for considering proper authentication options.
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Before a LAN is connected to the Internet, you need to determine what the access controls mechanisms are to be used, this would include how you are going to authenticate individuals that may access your network externally through access control.
The following answers are incorrect:
plan for implementing workstation locking mechanisms. This is incorrect because locking the workstations have no impact on the LAN or Internet access.
plan for protecting the modem pool. This is incorrect because protecting the modem pool has no impact on the LAN or Internet access, it just protects the modem.
plan for providing the user with his account usage information. This is incorrect because the question asks what should be done first. While important your primary concern should be focused on security.

NEW QUESTION: 289
A proxy is considered a:
A. first generation firewall.
B. third generation firewall.
C. second generation firewall.
D. fourth generation firewall.
Answer: (SHOW ANSWER)
Explanation/Reference:
The proxy (application layer firewall, circuit level proxy, or application proxy) is a second generation firewall
"First generation firewall" incorrect. A packet filtering firewall is a first generation firewall.
"Third generation firewall" is incorrect. Stateful Firewall are considered third generation firewalls
"Fourth generation firewall" is incorrect. Dynamic packet filtering firewalls are fourth generation firewalls
References:
CBK, p. 464
AIO3, pp. 482 - 484
Neither CBK or AIO3 use the generation terminology for firewall types but you will encounter it frequently as a practicing security professional. See http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm for a general discussion of the different generations.

NEW QUESTION: 290

In Discretionary Access Control the subject has authority, within certain limitations,
A. but he is not permitted to specify what objects can be accessible and so we need to get an independent third party to specify what objects can be accessible.
B. to specify what objects can be accessible.
C. to specify on a aggregate basis without understanding what objects can be accessible.
D. to specify in full detail what objects can be accessible.
Answer: (SHOW ANSWER)
Explanation/Reference:
With Discretionary Access Control, the subject has authority, within certain limitations, to specify what objects can be accessible.
For example, access control lists can be used. This type of access control is used in local, dynamic situations where the subjects must have the discretion to specify what resources certain users are permitted to access.
When a user, within certain limitations, has the right to alter the access control to certain objects, this is termed as user-directed discretionary access control. In some instances, a hybrid approach is used, which combines the features of user-based and identity-based discretionary access control.
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.
and
HARRIS, Shon, All-In-One CISSP Certification Exam Guide 5th Edition, McGraw-Hill/Osborne, 2010, Chapter 4: Access Control (page 210-211).

NEW QUESTION: 291
What kind of certificate is used to validate a user identity?
A. Public key certificate
B. Attribute certificate
C. Root certificate
D. Code signing certificate
Answer: A (LEAVE A REPLY)
Explanation/Reference:
In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.

In computer security, an authorization certificate (also known as an attribute certificate) is a digital document that describes a written permission from the issuer to use a service or a resource that the issuer controls or has access to use. The permission can be delegated.
Some people constantly confuse PKCs and ACs. An analogy may make the distinction clear. A PKC can be considered to be like a passport: it identifies the holder, tends to last for a long time, and should not be trivial to obtain. An AC is more like an entry visa: it is typically issued by a different authority and does not last for as long a time. As acquiring an entry visa typically requires presenting a passport, getting a visa can be a simpler process.
A real life example of this can be found in the mobile software deployments by large service providers and are typically applied to platforms such as Microsoft Smartphone (and related), Symbian OS, J2ME, and others.
In each of these systems a mobile communications service provider may customize the mobile terminal client distribution (ie. the mobile phone operating system or application environment) to include one or more root certificates each associated with a set of capabilities or permissions such as "update firmware", "access address book", "use radio interface", and the most basic one, "install and execute". When a developer wishes to enable distribution and execution in one of these controlled environments they must acquire a certificate from an appropriate CA, typically a large commercial CA, and in the process they usually have their identity verified using out-of-band mechanisms such as a combination of phone call, validation of their legal entity through government and commercial databases, etc., similar to the high assurance SSL certificate vetting process, though often there are additional specific requirements imposed on would-be developers/publishers.
Once the identity has been validated they are issued an identity certificate they can use to sign their software; generally the software signed by the developer or publisher's identity certificate is not distributed but rather it is submitted to processor to possibly test or profile the content before generating an authorization certificate which is unique to the particular software release. That certificate is then used with an ephemeral asymmetric key-pair to sign the software as the last step of preparation for distribution.
There are many advantages to separating the identity and authorization certificates especially relating to risk mitigation of new content being accepted into the system and key management as well as recovery from errant software which can be used as attack vectors.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 540.
http://en.wikipedia.org/wiki/Attribute_certificate
http://en.wikipedia.org/wiki/Public_key_certificate

NEW QUESTION: 292
This type of attack is generally most applicable to public-key cryptosystems, what type of attack am I ?
A. Chosen-Ciphertext attack
B. Ciphertext-only attack
C. Plaintext Only Attack
D. Adaptive-Chosen-Plaintext attack
Answer: A (LEAVE A REPLY)

Explanation/Reference:
A chosen-ciphertext attack is one in which cryptanalyst may choose a piece of ciphertext and attempt to obtain the corresponding decrypted plaintext. This type of attack is generally most applicable to public-key cryptosystems.
A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key. In the attack, an adversary has a chance to enter one or more known ciphertexts into the system and obtain the resulting plaintexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.
A number of otherwise secure schemes can be defeated under chosen-ciphertext attack. For example, the El Gamal cryptosystem is semantically secure under chosen-plaintext attack, but this semantic security can be trivially defeated under a chosen-ciphertext attack. Early versions of RSA padding used in the SSL protocol were vulnerable to a sophisticated adaptive chosen-ciphertext attack which revealed SSL session keys. Chosen-ciphertext attacks have implications for some self-synchronizing stream ciphers as well.
Designers of tamper-resistant cryptographic smart cards must be particularly cognizant of these attacks, as these devices may be completely under the control of an adversary, who can issue a large number of chosen-ciphertexts in an attempt to recover the hidden secret key.
According to RSA:
Cryptanalytic attacks are generally classified into six categories that distinguish the kind of information the cryptanalyst has available to mount an attack. The categories of attack are listed here roughly in increasing order of the quality of information available to the cryptanalyst, or, equivalently, in decreasing order of the level of difficulty to the cryptanalyst. The objective of the cryptanalyst in all cases is to be able to decrypt new pieces of ciphertext without additional information. The ideal for a cryptanalyst is to extract the secret key.
A ciphertext-only attack is one in which the cryptanalyst obtains a sample of ciphertext, without the plaintext associated with it. This data is relatively easy to obtain in many scenarios, but a successful ciphertext-only attack is generally difficult, and requires a very large ciphertext sample. Such attack was possible on cipher using Code Book Mode where frequency analysis was being used and even thou only the ciphertext was available, it was still possible to eventually collect enough data and decipher it without having the key.
A known-plaintext attack is one in which the cryptanalyst obtains a sample of ciphertext and the corresponding plaintext as well. The known-plaintext attack (KPA) or crib is an attack model for cryptanalysis where the attacker has samples of both the plaintext and its encrypted version (ciphertext), and is at liberty to make use of them to reveal further secret information such as secret keys and code books.
A chosen-plaintext attack is one in which the cryptanalyst is able to choose a quantity of plaintext and then obtain the corresponding encrypted ciphertext. A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further

information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key.
This appears, at first glance, to be an unrealistic model; it would certainly be unlikely that an attacker could persuade a human cryptographer to encrypt large amounts of plaintexts of the attacker's choosing. Modern cryptography, on the other hand, is implemented in software or hardware and is used for a diverse range of applications; for many cases, a chosen-plaintext attack is often very feasible. Chosen-plaintext attacks become extremely important in the context of public key cryptography, where the encryption key is public and attackers can encrypt any plaintext they choose.
Any cipher that can prevent chosen-plaintext attacks is then also guaranteed to be secure against known-plaintext and ciphertext-only attacks; this is a conservative approach to security.
Two forms of chosen-plaintext attack can be distinguished:
Batch chosen-plaintext attack, where the cryptanalyst chooses all plaintexts before any of them are encrypted. This is often the meaning of an unqualified use of "chosen-plaintext attack".
Adaptive chosen-plaintext attack, is a special case of chosen-plaintext attack in which the cryptanalyst is able to choose plaintext samples dynamically, and alter his or her choices based on the results of previous encryptions. The cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.
Non-randomized (deterministic) public key encryption algorithms are vulnerable to simple "dictionary"-type attacks, where the attacker builds a table of likely messages and their corresponding ciphertexts. To find the decryption of some observed ciphertext, the attacker simply looks the ciphertext up in the table. As a result, public-key definitions of security under chosen-plaintext attack require probabilistic encryption (i.e., randomized encryption). Conventional symmetric ciphers, in which the same key is used to encrypt and decrypt a text, may also be vulnerable to other forms of chosen-plaintext attack, for example, differential cryptanalysis of block ciphers.
An adaptive-chosen-ciphertext is the adaptive version of the above attack. A cryptanalyst can mount an attack of this type in a scenario in which he has free use of a piece of decryption hardware, but is unable to extract the decryption key from it.
An adaptive chosen-ciphertext attack (abbreviated as CCA2) is an interactive form of chosen-ciphertext attack in which an attacker sends a number of ciphertexts to be decrypted, then uses the results of these decryptions to select subsequent ciphertexts. It is to be distinguished from an indifferent chosen-ciphertext attack (CCA1).
The goal of this attack is to gradually reveal information about an encrypted message, or about the decryption key itself. For public-key systems, adaptive-chosen-ciphertexts are generally applicable only when they have the property of ciphertext malleability - that is, a ciphertext can be modified in specific ways that will have a predictable effect on the decryption of that message.
A Plaintext Only Attack is simply a bogus detractor. If you have the plaintext only then there is no need to perform any attack.
References:
RSA Laboratories FAQs about today's cryptography: What are some of the basic types of cryptanalytic attack?
also see:

http://www.giac.org/resources/whitepaper/cryptography/57.php
and
http://en.wikipedia.org/wiki/Chosen-plaintext_attack

NEW QUESTION: 293
Which ISO/OSI layer establishes the communications link between individual devices over a physical link or channel?
A. Transport layer
B. Network layer
C. Data link layer
D. Physical layer
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The data link layer (layer 2) establishes the communications link between individual devices over a physical link or channel. It also ensures that messages are delivered to the proper device and translates the messages from layers above into bits for the physical layer (layer 1) to transmit.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
83).

NEW QUESTION: 294
Which of the following firewall rules found on a firewall installed between an organization's internal network and the Internet would present the greatest danger to the internal network?
A. Permit all traffic between local hosts.
B. Permit all inbound ssh traffic.
C. Permit all inbound tcp connections.
D. Permit all syslog traffic to log-server.abc.org.
Answer: C (LEAVE A REPLY)
Any opening of an internal network to the Internet is susceptible of creating a new vulnerability.
Of the given rules, the one that permits all inbound tcp connections is the less likely to be used since it amounts to almost having no firewall at all, tcp being widely used on the Internet.
Reference(s) used for this question:
ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 409).

NEW QUESTION: 295
What attack involves the perpetrator sending spoofed packet(s) wich contains the same destination and source IP address as the remote host, the same port for the source and destination, having the SYN flag, and targeting any open ports that are open on the remote host?

A. Boink attack
B. Land attack
C. Teardrop attack
D. Smurf attack
Answer: (SHOW ANSWER)
The Land attack involves the perpetrator sending spoofed packet(s) with the SYN flag set to the victim's machine on any open port that is listening. The packet(s) contain the same destination and source IP address as the host, causing the victim's machine to reply to itself repeatedly. In addition, most systems experience a total freeze up, where as CTRL-ALT-DELETE fails to work, the mouse and keyboard become non operational and the only method of correction is to reboot via a reset button on the system or by turning the machine off.
The Boink attack, a modified version of the original Teardrop and Bonk exploit programs, is very similar to the Bonk attack, in that it involves the perpetrator sending corrupt UDP packets to the host. It however allows the attacker to attack multiple ports where Bonk was mainly directed to port 53 (DNS).
The Teardrop attack involves the perpetrator sending overlapping packets to the victim, when their machine attempts to re-construct the packets the victim's machine hangs.
A Smurf attack is a network-level attack against hosts where a perpetrator sends a large amount of ICMP echo (ping) traffic at broadcast addresses, all of it having a spoofed source address of a victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply each, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, there could potentially be hundreds of machines to reply to each packet.
Resources:
http://en.wikipedia.org/wiki/Denial-of-service_attack http://en.wikipedia.org/wiki/LAND

NEW QUESTION: 296
What is the Maximum Tolerable Downtime (MTD)?
A. Maximum elapsed time required to complete recovery of application data
B. Minimum elapsed time required to complete recovery of application data
C. Maximum elapsed time required to move back to primary site after a major disruption
D. It is maximum delay businesses can tolerate and still remain viable
Answer: D (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The Maximum Tolerable Downtime (MTD) is the maximum length of time a BUSINESS FUNCTION can endure without being restored, beyond which the BUSINESS is no longer viable NIST SAYS:
The ISCP Coordinator should analyze the supported mission/business processes and with the process owners, leadership and business managers determine the acceptable downtime if a given process or specific system data were disrupted or otherwise unavailable. Downtime can be identified in several ways.

Maximum Tolerable Downtime (MTD). The MTD represents the total amount of time the system owner/ authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on selection of an appropriate recovery method, and the depth of detail which will be required when developing recovery procedures, including their scope and content.
Other BCP and DRP terms you must be familiar with are:
Recovery Time Objective (RTO). RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/ business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.
Recovery Point Objective (RPO). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process. Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.
References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 276.
and
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

NEW QUESTION: 297
In a Public Key Infrastructure (PKI), what is the role of a directory server?
A. To make user certificates available to others
B. To issue certificates to users
C. Authorizes CA servers to issue certificates to users
D. Is the root authority for thePKI
Answer: A (LEAVE A REPLY)

NEW QUESTION: 298
Why do buffer overflows happen? What is the main cause?
A. Because buffers can only hold so much data
B. Because of improper parameter checking within the application
C. Because they are an easy weakness to exploit
D. Because of insufficient system memory
Answer: (SHOW ANSWER)

Section: Access Control
Explanation/Reference:
Buffer Overflow attack takes advantage of improper parameter checking within the application. This is the classic form of buffer overflow and occurs because the programmer accepts whatever input the user supplies without checking to make sure that the length of the input is less than the size of the buffer in the program.
The buffer overflow problem is one of the oldest and most common problems in software development and programming, dating back to the introduction of interactive computing. It can result when a program fills up the assigned buffer of memory with more data than its buffer can hold. When the program begins to write beyond the end of the buffer, the program's execution path can be changed, or data can be written into areas used by the operating system itself. This can lead to the insertion of malicious code that can be used to gain administrative privileges on the program or system.
As explained by Gaurab, it can become very complex. At the time of input even if you are checking the length of the input, it has to be check against the buffer size. Consider a case where entry point of data is stored in Buffer1 of Application1 and then you copy it to Buffer2 within Application2 later on, if you are just checking the length of data against Buffer1, it will not ensure that it will not cause a buffer overflow in Buffer2 of Application2.
A bit of reassurance from the ISC2 book about level of Coding Knowledge needed for the exam:
It should be noted that the CISSP is not required to be an expert programmer or know the inner workings of developing application software code, like the FORTRAN programming language, or how to develop Web applet code using Java. It is not even necessary that the CISSP know detailed security-specific coding practices such as the major divisions of buffer overflow exploits or the reason for preferring str(n)cpy to strcpy in the C language (although all such knowledge is, of course, helpful). Because the CISSP may be the person responsible for ensuring that security is included in such developments, the CISSP should know the basic procedures and concepts involved during the design and development of software programming. That is, in order for the CISSP to monitor the software development process and verify that security is included, the CISSP must understand the fundamental concepts of programming developments and the security strengths and weaknesses of various application development processes.
The following are incorrect answers:
"Because buffers can only hold so much data" is incorrect. This is certainly true but is not the best answer because the finite size of the buffer is not the problem -- the problem is that the programmer did not check the size of the input before moving it into the buffer.
"Because they are an easy weakness to exploit" is incorrect. This answer is sometimes true but is not the best answer because the root cause of the buffer overflow is that the programmer did not check the size of the user input.
"Because of insufficient system memory" is incorrect. This is irrelevant to the occurrence of a buffer overflow.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 13319-13323). Auerbach Publications. Kindle Edition.

NEW QUESTION: 299
Because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to:
A. neither physical attacks nor attacks from malicious code.
B. physical attacks only
C. both physical attacks and attacks from malicious code.
D. physical attacks but not attacks from malicious code.
Answer: C (LEAVE A REPLY)
Since all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to both physical attacks and attacks from malicious code.
Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

NEW QUESTION: 300
The term "principle of least privilege" is best as:
A. A separation of command, program and interface functions
B. Active monitoring with network base intrusion detection systems and host based intrusion detection systems
C. The process of granting each user the lowest clearance and access needed to accomplish their task
D. Implementation of mandatory access control
Answer: C (LEAVE A REPLY)
The principle of least privilege is used in part to limit the damage resulting from accidents, errors, or unauthorized use of system resources.

NEW QUESTION: 301
Which of the following is the primary reason why a user would choose a dial-up modem connection to the Internet when they have a faster, secure Internet connection through the organization's network?
A. To access web sites that blocked by the organization's proxy server.
B. To set up public services using the organization's resources.
C. To check their personal e-mail.
D. To circumvent the organization's security policy.
Answer: D (LEAVE A REPLY)
All the choices above represent examples of circumventing the organization's security policy, which is the primary reason why a user would be using a dial-up Internet connection when a secure connection is available through the organization's network.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1: Understanding Firewalls.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 302
While there are many different models for IT system life cycle most contain five unique phases. Which of the following would be the first phase?
A. Development
B. Initiation
C. Disposal
D. Operation / Maintenance
E. Implementation
Answer: B (LEAVE A REPLY)
The order of implementation is: initiation, development, implementation, operation/maintenance, and disposal.

NEW QUESTION: 303
Telnet and rlogin use which protocol?
A. UDP.
B. SNMP.
C. TCP.
D. IGP.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
TCP allows for reliabilty in connections which would be required for terminal emulation.
The following answers are incorrect:
UDP. Is incorrect because with User Datagram Protocol (UDP) you don't have a reliable transmission, datagrams could arrive out of sequence.
SNMP. Is incorrect because it is a network management protocol, Simple Network Management Protocol (SNMP).
IGP. Is incorrect because Interior Gateway Protocol (IGP) is used interally on a network.

NEW QUESTION: 304
When a station communicates on the network for the first time, which of the following protocol would search for and find the Internet Protocol (IP) address that matches with a known Ethernet address?

A. Address Resolution Protocol (ARP).
B. Reverse Address Resolution Protocol (RARP).
C. Internet Control Message protocol (ICMP).
D. User Datagram Protocol (UDP).
Answer: B (LEAVE A REPLY)
Explanation/Reference:
The RARP protocol sends out a packet, which includes its MAC address and a request to be informed of the IP address that should be assigned to that MAC address.
ARP does the opposite by broadcasting a request to find the Ethernet address that matches a known IP address.
ICMP supports packets containing error, control, and informational messages (e.g. PING).
UDP runs over IP and is used primarily for broadcasting messages over a network.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

NEW QUESTION: 305
Which TCSEC class specifies discretionary protection?
A. B2
B. B1
C. C2
D. C1
Answer: D (LEAVE A REPLY)
C1 involves discretionary protection, C2 involves controlled access protection, B1 involves labeled security protection and B2 involves structured protection. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 306
During the salvage of the Local Area Network and Servers, which of the following steps would normally be performed first?
A. Damage mitigation
B. Install LAN communications network and servers
C. Assess damage to LAN and servers
D. Recover equipment
Answer: (SHOW ANSWER)
The first activity in every recovery plan is damage assessment, immediately followed by damage mitigation.
This first activity would typically include assessing the damage to all network and server components (including cables, boards, file servers, workstations, printers, network equipment), making a list of all items to be repaired or replaced, selecting appropriate vendors and relaying findings to Emergency Management Team.

Following damage mitigation, equipment can be recovered and LAN communications network and servers can be reinstalled.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 135).

NEW QUESTION: 307
Secure Sockets Layer (SSL) is very heavily used for protecting which of the following?
A. Web transactions.
B. EDI transactions.
C. Telnet transactions.
D. Electronic Payment transactions.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
SSL was developed Netscape Communications Corporation to improve security and privacy of HTTP transactions.
SSL is one of the most common protocols used to protect Internet traffic.
It encrypts the messages using symmetric algorithms, such as IDEA, DES, 3DES, and Fortezza, and also calculates the MAC for the message using MD5 or SHA-1. The MAC is appended to the message and encrypted along with the message data.
The exchange of the symmetric keys is accomplished through various versions of Diffie-Hellmann or RSA.
TLS is the Internet standard based on SSLv3. TLSv1 is backward compatible with SSLv3. It uses the same algorithms as SSLv3; however, it computes an HMAC instead of a MAC along with other enhancements to improve security.
The following are incorrect answers:
"EDI transactions" is incorrect. Electronic Data Interchange (EDI) is not the best answer to this question though SSL could play a part in some EDI transactions.
"Telnet transactions" is incorrect. Telnet is a character mode protocol and is more likely to be secured by Secure Telnet or replaced by the Secure Shell (SSH) protocols.
"Eletronic payment transactions" is incorrect. Electronic payment is not the best answer to this question though SSL could play a part in some electronic payment transactions.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 16615-16619). Auerbach Publications. Kindle Edition.
and
http://en.wikipedia.org/wiki/Transport_Layer_Security

NEW QUESTION: 308
Which range defines "well known ports?"
A. 0-1024
B. 0-1023

C. 1024-49151
D. 1-1024
Answer: B (LEAVE A REPLY)

NEW QUESTION: 309
In which layer of the OSI Model are connection-oriented protocols located in the TCP/IP suite of protocols?
A. Transport layer
B. Application layer
C. Physical layer
D. Network layer
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Connection-oriented protocols such as TCP provides reliability.
It is the responsibility of such protocols in the transport layer to ensure every byte is accounted for. The network layer does not provide reliability. It only privides the best route to get the traffic to the final destination address.
For your exam you should know the information below about OSI model:
The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.
The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.
OSI Model
Image source: http://www.petri.co.il/images/osi_model.JPG
PHYSICAL LAYER
The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:
Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
What signal state represents a binary 1
How the receiving station knows when a "bit-time" starts
How the receiving station delimits a frame
DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.

Frame sequencing: transmits/receives frames sequentially.

Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame delimiting: creates and recognizes frame boundaries.

Frame error checking: checks received frames for integrity.

Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: routes frames among networks.

Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.

Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the

network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.

Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.

Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

The session layer allows session establishment between processes running on different stations. It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.

Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.

Data compression: reduces the number of bits that need to be transmitted on the network.

Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER
The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:
Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals
The following were incorrect answers:
Application Layer - The application layer serves as the window for users and application processes to access network services.
Network layer - The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.
Physical Layer - The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.
The following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 260
and
Official ISC2 guide to CISSP CBK 3rd Edition Page number 287
and
http://en.wikipedia.org/wiki/Tcp_protocol

NEW QUESTION: 310
Which of the following best ensures accountability of users for the actions taken within a system or domain?
A. Identification
B. Authentication
C. Authorization
D. Credentials
Answer: (SHOW ANSWER)
Details:
The only way to ensure accountability is if the subject is uniquely identified and authenticated. Identification alone does not provide proof the user is who they claim to be.
After showing proper credentials, a user is authorized access to resources.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002,

Chapter 4: Access Control (page 126).

NEW QUESTION: 311
Which of the following is needed for System Accountability?
A. Audit mechanisms.
B. Documented design as laid out in the Common Criteria.
C. Authorization.
D. Formal verification of system design.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Is a means of being able to track user actions. Through the use of audit logs and other tools the user actions are recorded and can be used at a later date to verify what actions were performed.
Accountability is the ability to identify users and to be able to track user actions.
The following answers are incorrect:
Documented design as laid out in the Common Criteria. Is incorrect because the Common Criteria is an international standard to evaluate trust and would not be a factor in System Accountability.
Authorization. Is incorrect because Authorization is granting access to subjects, just because you have authorization does not hold the subject accountable for their actions.
Formal verification of system design. Is incorrect because all you have done is to verify the system design and have not taken any steps toward system accountability.
References:
OIG CBK Glossary (page 778)

NEW QUESTION: 312
Which of the following is an example of a connectionless communication protocol?
A. UDP
B. X.25
C. Packet switching
D. TCP
Answer: A (LEAVE A REPLY)
Explanation/Reference:
UDP is an example of connectionless communication protocol, wherein no connection needs to be established before data can be exchanged.
In telecommunications, connectionless describes communication between two network end points in which a message can be sent from one end point to another without prior arrangement. The device at one end of the communication transmits data addressed to the other, without first ensuring that the recipient is available and ready to receive the data. Some protocols allow for error correction by requested retransmission. Internet Protocol (IP) and User Datagram Protocol (UDP) are connectionless protocols.
Connectionless protocols are also described as stateless because the endpoints have no protocol-defined way to remember where they are in a "conversation" of message exchanges.

List of connectionless protocols
Hypertext Transfer Protocol
IP
UDP
ICMP
IPX
TIPC
NetBEUI
References:
KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 86).
and
https://secure.wikimedia.org/wikipedia/en/wiki/Connectionless_protocol

NEW QUESTION: 313
Which of the following transmission media would NOT be affected by cross talk or interference?
A. Copper cable
B. Radio System
C. Satellite radiolink
D. Fiber optic cables
Answer: D (LEAVE A REPLY)
Only fiber optic cables are not affected by crosstalk or interference.
For your exam you should know the information about transmission media:
Copper Cable Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data. Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.
Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.
Copper Cable
Image Source http://i00.i.aliimg.com/photo/v0/570456138/FRLS_HR_PVC_Copper_Cable.jpg
Coaxial cable Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of

the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.
Coaxial cable are expensive and does not support many LAN's. It supports data and video Coaxial Cable
Image Source - http://www.tlc-direct.co.uk/Images/Products/size_3/CARG59.JPG
Fiber optics
An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.
Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.
Radio System
Radio systems are used for short distance,cheap and easy to tap.
Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.
Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width.
When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.
Fiber Optics
Image Source - http://aboveinfranet.com/wp-content/uploads/2014/04/fiber-optic-cablesabove-infranet-solutions.jpg
Microwave radio system Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimetre; these are called microwaves. Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.
Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.
Microwave radio systems are carriers for voice data signal, cheap and easy to tap.
Microwave Radio System

Image Source http://www.valiantcom.com/images/applications/e1_digital_microwave_radio.gif
Satellite Radio Link Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.
Satellite radio link uses transponder to send information and easy to tap.
The following answers are incorrect:
Copper Cable - Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Radio System - Radio systems are used for short distance,cheap and easy to tap.
Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.
The following reference(s) were/was used to create this question:
CISA review manual 2014 page number 265 &
Official ISC2 guide to CISSP CBK 3rd Edition Page number 233

NEW QUESTION: 314
Which of the following was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support?
A. SESAME
B. RADIUS
C. KryptoKnight
D. TACACS+
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Secure European System for Applications in a Multi-vendor Environment (SESAME) was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support.
Reference:
TIPTON, Harold, Official (ISC)2 Guide to the CISSP CBK (2007), page 184.
ISC OIG Second Edition, Access Controls, Page 111

NEW QUESTION: 315
Which of the following offers security to wireless communications?
A. S-WAP
B. WTLS
C. WSP
D. WDP
Answer: B (LEAVE A REPLY)
Explanation/Reference:

Wireless Transport Layer Security (WTLS) is a communication protocol that allows wireless devices to send and receive encrypted information over the Internet. S-WAP is not defined. WSP (Wireless Session Protocol) and WDP (Wireless Datagram Protocol) are part of Wireless Access Protocol (WAP).
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 173).

NEW QUESTION: 316
Which of the following is an IP address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?
A. 172.12.42.5
B. 172.140.42.5
C. 172.31.42.5
D. 172.15.42.5
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
This is a valid Class B reserved address. For Class B networks, the reserved addresses are 172.16.0.0 - 172.31.255.255.
The private IP address ranges are defined within RFC 1918:
RFC 1918 private ip address range
The following answers are incorrect:
172.12.42.5 Is incorrect because it is not a Class B reserved address.
172.140.42.5 Is incorrect because it is not a Class B reserved address.
172.15.42.5 Is incorrect because it is not a Class B reserved address.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 317
When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?
A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.

C. They both involve rewriting the media.
D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack). There are three general methods of purging media: overwriting, degaussing, and destruction.
There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.
Reference(s) use for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 26).
and
A guide to understanding Data Remanence in Automated Information Systems

NEW QUESTION: 318
The IP header contains a protocol field. If this field contains the value of 17, what type of data is contained within the ip datagram?
A. TCP.
B. ICMP.
C. UDP.
D. IGMP.
Answer: C (LEAVE A REPLY)
If the protocol field has a value of 17 then it would indicate it was UDP.
The following answers are incorrect answers:
TCP. Is incorrect because the value for a TCP protocol would be 6. ICMP. Is incorrect because the value for an ICMP protocol would be 1. IGMP. Is incorrect because the value for an IGMP protocol would be 2.
The protocol field of the IP packet dictates what protocol the IP packet is using. TCP=6, ICMP=1, UDP=17, IGMP=2
Reference(s) used for this question:
SANS http://www.sans.org/resources/tcpip.pdf?ref=3871

NEW QUESTION: 319

Which of the following is used in database information security to hide information?
A. Inheritance
B. Polyinstantiation
C. Polymorphism
D. Delegation
Answer: (SHOW ANSWER)
Explanation/Reference:
Polyinstantiation enables a relation to contain multiple tuples with the same primary keys with each instance distinguished by a security level. When this information is inserted into a database, lower-level subjects need to be restricted from this information. Instead of just restricting access, another set of data is created to fool the lower-level subjects into thinking that the information actually means something else.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter
11: Application and System Development (page 727).

NEW QUESTION: 320
Which of the following is a trusted, third party authentication protocol that was developed under Project Athena at MIT?
A. Kerberos
B. SESAME
C. KryptoKnight
D. NetSP
Answer: (SHOW ANSWER)
Explanation/Reference:
Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT.
Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/ server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.
The Internet is an insecure place. Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by systems crackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, other client/ server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server.
Some sites attempt to use firewalls to solve their network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a very bad assumption. Most of the really damaging incidents of computer crime are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict how your users can use the Internet. (After all, firewalls are simply a less extreme example of the dictum that there is nothing more secure then a computer which is not

connected to the network --- and powered off!) In many places, these restrictions are simply unrealistic and unacceptable.
Kerberos was created by MIT as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.
Kerberos is freely available from MIT, under a copyright permission notice very similar to the one used for the BSD operating and X11 Windowing system. MIT provides Kerberos in source form, so that anyone who wishes to use it may look over the code for themselves and assure themselves that the code is trustworthy.
In addition, for those who prefer to rely on a professional supported product, Kerberos is available as a product from many different vendors.
In summary, Kerberos is a solution to your network security problems. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. We hope you find Kerberos as useful as it has been to us. At MIT, Kerberos has been invaluable to our Information/Technology architecture.
KryptoKnight is a Peer to Peer authentication protocol incorporated into the NetSP product from IBM.
SESAME is an authentication and access control protocol, that also supports communication confidentiality and integrity. It provides public key based authentication along with the Kerberos style authentication, that uses symmetric key cryptography. Sesame supports the Kerberos protocol and adds some security extensions like public key based authentication and an ECMA-style Privilege Attribute Service. The complete Sesame protocol is a two step process. In the first step, the client successfully authenticates itself to the Authentication Server and obtains a ticket that can be presented to the Privilege Attribute Server. In the second step, the initiator obtains proof of his access rights in the form of Privilege Attributes Certificate (PAC). The PAC is a specific form of Access Control Certificate as defined in the ECMA-219 document. This document describes the extensions to Kerberos for public key based authentication as adopted in Sesame.
SESAME, KryptoKnight, and NetSP never took off and the protocols are no longer commonly used.
References:
http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#whatis
and
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 40.

NEW QUESTION: 321
Which of the following attacks could capture network user passwords?
A. Data diddling
B. Sniffing
C. IP Spoofing
D. Smurfing

Answer: (SHOW ANSWER)

A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.

Sniffers are typically devices that can collect information from a communication medium, such as a network. These devices can range from specialized equipment to basic workstations with customized software.

A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch. A hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in.

Another method for sniffing is to use a network tap-a device that literally splits a network transmission into two identical streams; one going to the original network destination and the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity.

The packets captured by sniffer are decoded and then displayed by the sniffer. Therfore, if the username/password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that segment it can see).

Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.

The following answers are incorrect:

Data diddling involves changing data before, as it is enterred into a computer, or after it is extracted.

Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.

Smurfing would refer to the smurf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.

The following reference(s) were/was used to create this question:

CISA Review manual 2014 Page number 321 Official ISC2 Guide to the CISSP 3rd edition Page Number 153

NEW QUESTION: 322

Which of the following statements pertaining to biometrics is false?

A. Increased system sensitivity can cause a higher false rejection rate

B. The crossover error rate is the point at which false rejection rate equals the false acceptance rate.

C. False acceptance rate is also known as Type II error.

D. Biometrics are based on the Type 2 authentication mechanism.

Answer: D (LEAVE A REPLY)
Explanation/Reference:
Authentication is based on three factor types: type 1 is something you know, type 2 is something you have and type 3 is something you are. Biometrics are based on the Type 3 authentication mechanism.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 37).

NEW QUESTION: 323
SATAN stands for _____
A. Scavanger Administrator Tool for Analyzing Networks
B. Storage Administration Tool for Analyzing Networks
C. Simple Administration Tool for Analyzing Networks
D. System Administrator Tool for Analyzing Networks
E. SANS Administrator Tool for Analyzing Networks
F. Security Administrator Tool for Analyzing Networks
Answer: F (LEAVE A REPLY)
: . SATAN (an acronym standing for Security Administrator Tool for Analyzing Networks) is a testing and reporting tool that gathers information from networks, such as type of machine and security flaws that may be on these machines. SATAN was developed by Dan Farmer of Silicon Graphics with a purpose of scanning thousands of host computers on the Internet for security vulnerabilities. Availability: anonymous ftp at ftp.cerias.purdue.edu

NEW QUESTION: 324
What is the greatest danger from DHCP?
A. An intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients.
B. Having multiple clients on the same LAN having the same IP address.
C. Having the wrong router used as the default gateway.
D. Having the organization's mail server unreachable.
Answer: (SHOW ANSWER)
Explanation/Reference:
The greatest danger from BootP or DHCP (Dynamic Host Control Protocol) is from an intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients. Other choices are possible consequences of DHCP impersonation.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 4: Sockets and Services from a Security Viewpoint.

NEW QUESTION: 325
What does "System Integrity" mean?
A. The software of the system has been implemented as designed.
B. Users can't tamper with processes they do not own.

C. Hardware and firmware have undergone periodic testing to verify that they are functioning properly.
D. Design specifications have been verified against the formal top-level specification.
Answer: C (LEAVE A REPLY)
System Integrity means that all components of the system cannot be
tampered with by unauthorized personnel and can be verified that they work properly.
The following answers are incorrect:
The software of the system has been implemented as designed. Is incorrect because this
would fall under Trusted system distribution.
Users can't tamper with processes they do not own. Is incorrect because this would fall
under Configuration Management.
Design specifications have been verified against the formal top-level specification. Is
incorrect because this would fall under Specification and verification.
References:
AIOv3 Security Models and Architecture (pages 302 - 306)
DOD TCSEC - http://www.cerberussystems.com/INFOSEC/stds/d520028.htm

NEW QUESTION: 326
An effective information security policy should not have which of the following characteristic?
A. Include separation of duties
B. Be designed with a short- to mid-term focus
C. Be understandable and supported by all stakeholders
D. Specify areas of responsibility and authority
Answer: B (LEAVE A REPLY)
Explanation/Reference:
An effective information security policy should be designed with a long-term focus. All other
characteristics apply.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley,
2001, Appendix B, Practice-Level Policy Considerations (page 397).

NEW QUESTION: 327
One of the following statements about the differences between PPTP and L2TP is NOT true
A. PPTP can run only on top of IP networks.
B. PPTP is an encryption protocol and L2TP is not.
C. L2TP works well with all firewalls and network devices that perform NAT.
D. L2TP supports AAA servers
Answer: C (LEAVE A REPLY)
Explanation/Reference:
L2TP is affected by packet header modification and cannot cope with firewalls and network devices that
perform NAT.
"PPTP can run only on top of IP networks." is correct as PPTP encapsulates datagrams into an IP
packet, allowing PPTP to route many network protocols across an IP network.

"PPTP is an encryption protocol and L2TP is not." is correct. When using PPTP, the PPP payload is encrypted with Microsoft Point-to-Point Encryption (MPPE) using MSCHAP or EAP-TLS.
"L2TP supports AAA servers" is correct as L2TP supports TACACS+ and RADIUS.
NOTE:
L2TP does work over NAT. It is possible to use a tunneled mode that wraps every packet into a UDP packet. Port 4500 is used for this purpose. However this is not true of PPTP and it is not true as well that it works well with all firewalls and NAT devices.
References:
All in One Third Edition page 545
Official Guide to the CISSP Exam page 124-126

NEW QUESTION: 328
In computing what is the name of a non-self-replicating type of malware program containing malicious code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it, when executed, carries out actions that are unknown to the person installing it, typically causing loss or theft of data, and possible system harm.
A. virus
B. worm
C. Trojan horse.
D. trapdoor
Answer: (SHOW ANSWER)
A trojan horse is any code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it. A Trojan often also includes a trapdoor as a means to gain access to a computer system bypassing security controls.
Wikipedia defines it as: A Trojan horse, or Trojan, in computing is a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. The term is derived from the story of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece, because computer Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.
The following answers are incorrect: virus. Is incorrect because a Virus is a malicious program and is does not appear to be harmless, it's sole purpose is malicious intent often doing damage to a system. A computer virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected".
worm. Is incorrect because a Worm is similiar to a Virus but does not require user intervention to execute. Rather than doing damage to the system, worms tend to self-propagate and devour the resources of a system. A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing

program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
trapdoor. Is incorrect because a trapdoor is a means to bypass security by hiding an entry point into a system. Trojan Horses often have a trapdoor imbedded in them.
References:
http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29 and
http://en.wikipedia.org/wiki/Computer_virus and http://en.wikipedia.org/wiki/Computer_worm and
http://en.wikipedia.org/wiki/Backdoor_%28computing%29

NEW QUESTION: 329
Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?
A. B
B. A
C. C
D. D
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
B level is the first Mandatory Access Control Level.
First published in 1983 and updated in 1985, the TCSEC, frequently referred to as the Orange Book, was a United States Government Department of Defense (DoD) standard that sets basic standards for the implementation of security protections in computing systems. Primarily intended to help the DoD find products that met those basic standards, TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information on military and government systems. As such, it was strongly focused on enforcing confidentiality with no focus on other aspects of security such as integrity or availability. Although it has since been superseded by the common criteria, it influenced the development of other product evaluation criteria, and some of its basic approach and terminology continues to be used.
Reference used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17920-17926). Auerbach Publications. Kindle Edition.
and
THE source for all TCSEC "level" questions: http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt (paragraph 3 for this one)

NEW QUESTION: 330
Which of the following statements pertaining to biometrics is false?
A. Increased system sensitivity can cause a higher false rejection rate
B. The crossover error rate is the point at which false rejection rate equals the false acceptance rate.
C. False acceptance rate is also known as Type II error.

D. Biometrics are based on the Type 2 authentication mechanism.
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Authentication is based on three factor types: type 1 is something you know, type 2 is something you have and type 3 is something you are. Biometrics are based on the Type 3 authentication mechanism.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 37).

NEW QUESTION: 331
Which of the following is implemented through scripts or smart agents that replays the users multiple log-ins against authentication servers to verify a user's identity which permit access to system services?
A. Single Sign-On
B. Dynamic Sign-On
C. Smart cards
D. Kerberos
Answer: (SHOW ANSWER)
SSO can be implemented by using scripts that replay the users multiple log-
ins against authentication servers to verify a user's identity and to permit access to system services.
Single Sign on was the best answer in this case because it would include Kerberos.
When you have two good answers within the 4 choices presented you must select the BEST one. The high level choice is always the best. When one choice would include the other one that would be the best as well.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 40.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 332
Which security model ensures that actions that take place at a higher security level do not affect actions that take place at a lower level?
A. The Bell-LaPadula model

B. The information flow model
C. The noninterference model
D. The Clark-Wilson model
Answer: C (LEAVE A REPLY)
Explanation/Reference:
The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users, By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.
The model ensures that any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level.
It is not concerned with the flow of data, but rather with what a subject knows about the state of the system. So if an entity at a higher security level performs an action, it can not change the state for the entity at the lower level.
The model also addresses the inference attack that occurs when some one has access to some type of information and can infer(guess) something that he does not have the clearance level or authority to know.
The following are incorrect answers:
The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned only with confidentiality and bases access control decisions on the classfication of objects and the clearences of subjects.
The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security classes. Information will be allowed to flow only in accordance with the security policy.
The Clark-Wilson model is incorrect. The Clark-Wilson model is concerned with change control and assuring that all modifications to objects preserve integrity by means of well-formed transactions and usage of an access triple (subjet - interface - object).
References:
CBK, pp 325 - 326
AIO3, pp. 290 - 291
AIOv4 Security Architecture and Design (page 345)
AIOv5 Security Architecture and Design (pages 347 - 348)
https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Models#Noninterference_Models

NEW QUESTION: 333
What can be defined as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity?
A. A digital envelope
B. A cryptographic hash
C. A Message Authentication Code
D. A digital signature
Answer: D (LEAVE A REPLY)

Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines a digital signature as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.
The steps to create a Digital Signature are very simple:
1. You create a Message Digest of the message you wish to send
2. You encrypt the message digest using your Private Key which is the action of Signing
3. You send the Message along with the Digital Signature to the recipient To validate the Digital Signature the recipient will make use of the sender Public Key. Here are the steps:
1. The receiver will decrypt the Digital Signature using the sender Publick Key producing a clear text message digest.
2. The receiver will produce his own message digest of the message received.
3. At this point the receiver will compare the two message digest (the one sent and the one produce by the receiver), if the two matches, it proves the authenticity of the message and it confirms that the message was not modified in transit validating the integrity as well. Digital Signatures provides for Authenticity and Integrity only. There is no confidentiality in place, if you wish to get confidentiality it would be needed for the sender to encrypt everything with the receiver public key as a last step before sending the message.
A Digital Envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient. In simple term it is a type of security that uses two layers of encryption to protect a message. First, the message itself is encoded using symmetric encryption, and then the key to decode the message is encrypted using public-key encryption. This technique overcomes one of the problems of public-key encryption, which is that it is slower than symmetric encryption. Because only the key is protected with public-key encryption, there is very little overhead.
A cryptographic hash is the result of a cryptographic hash function such as MD5, SHA-1, or SHA-2. A hash value also called a Message Digest is like a fingerprint of a message. It is used to proves integrity and ensure the message was not changed either in transit or in storage.
A Message Authentication Code (MAC) refers to an ANSI standard for a checksum that is computed with a keyed hash that is based on DES or it can also be produced without using DES by concataning the Secret Key at the end of the message (simply adding it at the end of the message) being sent and then producing a Message digest of the Message+Secret Key together. The MAC is then attached and sent along with the message but the Secret Key is NEVER sent in clear text over the network.
In cryptography, HMAC (Hash-based Message Authentication Code), is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly.
The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output length in bits and on the size and quality of the cryptographic key.
There is more than one type of MAC: Meet CBC-MAC

In cryptography, a Cipher Block Chaining Message Authentication Code, abbreviated CBC-MAC, is a technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the previous block. This interdependence ensures that a change to any of the plaintext bits will cause the final encrypted block to change in a way that cannot be predicted or counteracted without knowing the key to the block cipher.
References:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
http://www.webopedia.com/TERM/D/digital_envelope.html
and
http://en.wikipedia.org/wiki/CBC-MAC

NEW QUESTION: 334
What is called an event or activity that has the potential to cause harm to the information systems or networks?
A. Vulnerability
B. Threat agent
C. Weakness
D. Threat
Answer: D (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

NEW QUESTION: 335
What is the proper term to refer to a single unit of Ethernet data at the link layer of the DoD TCP model ?
A. Ethernet Segment.
B. Ethernet Datagram.
C. Ethernet Frame.
D. Ethernet Packet.
Answer: (SHOW ANSWER)
Ethernet is frame based network technology. See below a few definitions from RFC 1122:
SEGMENT A segment is the unit of end-to-end transmission in the TCP protocol. A segment consists of a TCP header followed by application data. A segment is transmitted by encapsulation inside an IP datagram.
PACKET A packet is the unit of data passed across the interface between the internet layer and the link layer. It includes an IP header and data. A packet may be a complete IP datagram or a fragment of an IP datagram.

FRAME A frame is the unit of transmission in a link layer protocol, and consists of a link-layer header followed by a packet.
The following answers are incorrect:
Ethernet segment. Is incorrect because Ethernet segment is a distractor, TCP segment would be the correct terminology. Ethernet is a frame based network technology,
Ethernet datagram. Is incorrect because Ethernet datagram is a distractor, IP datagram would be the correct terminology. Ethernet is a frame based network technology
Ethernet packet. Is incorrect because Ethernet packet is a distractor, a Packet is a group of information so would not be a "single unit". Ethernet is a frame based network technology.
Look at the diagrams below that were extracted from my Security+ Computer Based Tutorial. TCP/IP Data Structures
IMPORTANT NOTE:
The names used on the diagram above are from RFC 1122 which describe the DOD
Model.
Vendors and Books may use slightly different names or even number of layers.
TCP/IP Data Structure The following Reference(s) were used for this question:
Wikipedia http://en.wikipedia.org/wiki/Ethernet

NEW QUESTION: 336
What happens if this registry value is set to 1? HKLM\System\CurrentControlSet\Control\Lsa \CrashonAuditFail
A. System will continue operations as normal
B. System will crash
C. System will overwrite logs
D. System will perform a shutdown if maximum log size is reached
E. No such registry key exists
Answer: (SHOW ANSWER)

NEW QUESTION: 337
What attribute is included in a X.509-certificate?
A. Distinguished name of the subject
B. Telephone number of the department
C. secret key of the issuing CA
D. the key pair of the certificate holder
Answer: A (LEAVE A REPLY)
RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile; GUTMANN, P., X.509 style guide; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

NEW QUESTION: 338
Which of the following methods of providing telecommunications continuity involves the use of an alternative media?

A. Alternative routing
B. Diverse routing
C. Long haul network diversity
D. Last mile circuit protection
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Alternative routing is a method of routing information via an alternate medium such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network be unavailable.
Diverse routing routes traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and therefore subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. This type of access is time-consuming and costly. Long haul network diversity is a diverse long-distance network utilizing T1 circuits among the major long-distance carriers. It ensures long-distance access should any one carrier experience a network failure.
Last mile circuit protection is a redundant combination of local carrier T1s microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing is also utilized.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 259).

NEW QUESTION: 339
What does the (star) property mean in the Bell-LaPadula model?
A. No write up
B. No read up
C. No write down
D. No read down
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The (star) property of the Bell-LaPadula access control model states that writing of information by a subject at a higher level of sensitivity to an object at a lower level of sensitivity is not permitted (no write down).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 202).
Also check out: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 5: Security Models and Architecture (page 242, 243).

NEW QUESTION: 340
Brute force attacks against encryption keys have increased in potency because of increased computing power.
Which of the following is often considered a good protection against the brute force cryptography attack?
A. The use of good key generators.
B. The use of session keys.
C. Nothing can defend you against a brute force crypto key attack.
D. Algorithms that are immune to brute force key attacks.
Answer: B (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
If we assume a crytpo-system with a large key (and therefore a large key space) a brute force attack will likely take a good deal of time - anywhere from several hours to several years depending on a number of variables. If you use a session key for each message you encrypt, then the brute force attack provides the attacker with only the key for that one message. So, if you are encrypting 10 messages a day, each with a different session key, but it takes me a month to break each session key then I am fighting a loosing battle.
The other answers are not correct because:
"The use of good key generators" is not correct because a brute force key attack will eventually run through all possible combinations of key. Therefore, any key will eventually be broken in this manner given enough time.
"Nothing can defend you against a brute force crypto key attack" is incorrect, and not the best answer listed.
While it is technically true that any key will eventually be broken by a brute force attack, the question remains
"how long will it take?". In other words, if you encrypt something today but I can't read it for 10,000 years, will you still care? If the key is changed every session does it matter if it can be broken after the session has ended? Of the answers listed here, session keys are "often considered a good protection against the brute force cryptography attack" as the question asks.
"Algorithms that are immune to brute force key attacks" is incorrect because there currently are no such algorithms.
References:
Official ISC2 Guide page: 259
All in One Third Edition page: 623

NEW QUESTION: 341
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system. Acceptable throughput rates are in the range of:
A. 100 subjects per minute.
B. 25 subjects per minute.

C. 10 subjects per minute.
D. 50 subjects per minute.
Answer: C (LEAVE A REPLY)
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system.
Acceptable throughput rates are in the range of 10 subjects per minute.
Things that may impact the throughput rate for some types of biometric systems may include:
A concern with retina scanning systems may be the exchange of body fluids on the eyepiece.
Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

NEW QUESTION: 342
What does it mean to say that sensitivity labels are "incomparable"?
A. The number of classification in the two labels is different.
B. Neither label contains all the classifications of the other.
C. the number of categories in the two labels are different.
D. Neither label contains all the categories of the other.
Answer: D (LEAVE A REPLY)
If a category does not exist then you cannot compare it. Incomparable is when you have two disjointed sensitivity labels, that is a category in one of the labels is not in the other label. "Because neither label contains all the categories of the other, the labels can't be compared. They're said to be incomparable"
COMPARABILITY:
The label:
TOP SECRET [VENUS ALPHA]
is "higher" than either of the labels:
SECRET [VENUS ALPHA] TOP SECRET [VENUS]
But you can't really say that the label:
TOP SECRET [VENUS]
is higher than the label:
SECRET [ALPHA]
Because neither label contains all the categories of the other, the labels can't be compared. They're said to be incomparable. In a mandatory access control system, you won't be allowed access to a file whose label is incomparable to your clearance.
The Multilevel Security policy uses an ordering relationship between labels known as the dominance relationship. Intuitively, we think of a label that dominates another as being "higher" than the other. Similarly, we think of a label that is dominated by another as being

"lower" than the other. The dominance relationship is used to determine permitted operations and information flows.
DOMINANCE
The dominance relationship is determined by the ordering of the Sensitivity/Clearance component of the label and the intersection of the set of Compartments.
Sample Sensitivity/Clearance ordering are:
Top Secret > Secret > Confidential > Unclassified
s3 > s2 > s1 > s0
Formally, for label one to dominate label 2 both of the following must be true:
The sensitivity/clearance of label one must be greater than or equal to the sensitivity/clearance of label two.
The intersection of the compartments of label one and label two must equal the compartments of label two.
Additionally:
Two labels are said to be equal if their sensitivity/clearance and set of compartments are exactly equal. Note that dominance includes equality.
One label is said to strictly dominate the other if it dominates the other but is not equal to the other.
Two labels are said to be incomparable if each label has at least one compartment that is not included in the other's set of compartments.
The dominance relationship will produce a partial ordering over all possible MLS labels, resulting in what is known as the MLS Security Lattice.
The following answers are incorrect:
The number of classification in the two labels is different. Is incorrect because the categories are what is being compared, not the classifications.
Neither label contains all the classifications of the other. Is incorrect because the categories are what is being compared, not the classifications.
the number of categories in the two labels is different. Is incorrect because it is possibe a category exists more than once in one sensitivity label and does exist in the other so they would be comparable.
Reference(s) used for this question:
OReilly - Computer Systems and Access Control (Chapter 3)
http://www.oreilly.com/catalog/csb/chapter/ch03.html
and
http://rubix.com/cms/mls_dom

NEW QUESTION: 343
Which of the following should NOT be performed by an operator?
A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry

D. Controlling job flow

E. Section: Security Operation Adimnistration

Explanation/Reference:

Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel.

System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs. Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system's security policy. As such, use of these privileges should be monitored through audit logs.

Some of the privileges and responsibilities assigned to operators include:

Implementing the initial program load: This is used to start the operating system. The boot process or initial program load of a system is a critical time for ensuring system security. Interruptions to this process may reduce the integrity of the system or cause the system to crash, precluding its availability.

Monitoring execution of the system: Operators respond to various events, to include errors, interruptions, and job completion messages.

Volume mounting: This allows the desired application access to the system and its data.

Controlling job flow: Operators can initiate, pause, or terminate programs. This may allow an operator to affect the scheduling of jobs. Controlling job flow involves the manipulation of configuration information needed by the system. Operators with the ability to control a job or application can cause output to be altered or diverted, which can threaten the confidentiality.

Bypass label processing: This allows the operator to bypass security label information to run foreign tapes (foreign tapes are those from a different data center that would not be using the same label format that the system could run). This privilege should be strictly controlled to prevent unauthorized access.

Renaming and relabeling resources: This is sometimes necessary in the mainframe environment to allow programs to properly execute. Use of this privilege should be monitored, as it can allow the unauthorized viewing of sensitive information.

Reassignment of ports and lines: Operators are allowed to reassign ports or lines. If misused, reassignment can cause program errors, such as sending sensitive output to an unsecured location. Furthermore, an incidental port may be opened, subjecting the system to an attack through the creation of a new entry point into the system.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 19367-19395). Auerbach Publications. Kindle Edition.

129

Which of the following should be performed by an operator?

A. Changing profiles

B. Approving changes

C. Adding and removal of users

D. Installing system software

Answer: C (LEAVE A REPLY)

Of the listed tasks, installing system software is the only task that should normally be performed by an operator in a properly segregated environment.

Source: MOSHER, Richard & ROTHKE, Ben, CISSP CBK Review presentation on domain 7.

NEW QUESTION: 344

What is NOT an authentication method within IKE and IPsec?

A. CHAP

B. Pre shared key

C. certificate based authentication

D. Public key authentication

Answer: A (LEAVE A REPLY)

CHAP is not used within IPSEC or IKE. CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password).

After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.

The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.

The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.

At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.

The following were incorrect answers:

Pre Shared Keys

In cryptography, a pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. To build a key from shared secret, the key derivation function should be used. Such systems almost always use symmetric key cryptographic algorithms. The term PSK is used in WiFi encryption such as WEP or WPA, where both the wireless access points (AP) and all clients share the same key.

The characteristics of this secret or key are determined by the system which uses it; some system designs require that such keys be in a particular format. It can be a password like 'bret13i', a passphrase like 'Idaho hung gear id gene', or a hexadecimal string like '65E4 E556 8622 EEE1'. The secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems.

Certificat Based Authentication

The most common form of trusted authentication between parties in the wide world of Web commerce is the exchange of certificates. A certificate is a digital document that at a minimum includes a Distinguished Name (DN) and an associated public key.

The certificate is digitally signed by a trusted third party known as the Certificate Authority (CA). The CA vouches for the authenticity of the certificate holder. Each principal in the transaction presents certificate as its credentials. The recipient then validates the certificate's signature against its cache of known and trusted CA certificates. A "personal certificate" identifies an end user in a transaction; a "server certificate" identifies the service provider.

Generally, certificate formats follow the X.509 Version 3 standard. X.509 is part of the Open Systems Interconnect

(OSI) X.500 specification.

Public Key Authentication

Public key authentication is an alternative means of identifying yourself to a login server, instead of typing a password. It is more secure and more flexible, but more difficult to set up.

In conventional password authentication, you prove you are who you claim to be by proving that you know the correct password. The only way to prove you know the password is to tell the server what you think the password is. This means that if the server has been hacked, or spoofed an attacker can learn your password.

Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have a copy of that private key; but anybody who has your public key can verify that a particular signature is genuine.

So you generate a key pair on your own computer, and you copy the public key to the server. Then, when the server asks you to prove who you are, you can generate a signature using your private key. The server can verify that signature (since it has your public key) and allow you to log in. Now if the server is hacked or spoofed, the attacker does not gain your private key or password; they only gain one signature. And signatures cannot be re-used, so they have gained nothing.

There is a problem with this: if your private key is stored unprotected on your own computer, then anybody who gains access to your computer will be able to generate signatures as if they were you. So they will be able to log in to your server under your account. For this reason, your private key is usually encrypted when it is stored on your local machine, using a passphrase of your choice. In order to generate a signature, you must decrypt the key, so you have to type your passphrase.

References:

RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand & HARKINS, Dan

Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E.
Internet Cryptography, 1997, Addison-Wesley Pub Co.; HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 467.
http://en.wikipedia.org/wiki/Pre-shared_key
http://www.home.umk.pl/~mgw/LDAP/RS.C4.JUN.97.pdf
http://the.earth.li/~sgtatham/putty/0.55/htmldoc/Chapter8.html#S8.1

NEW QUESTION: 345
Which of the following was designed to support multiple network types over the same serial link?
A. Ethernet
B. SLIP
C. PPP
D. PPTP
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The Point-to-Point Protocol (PPP) was designed to support multiple network types over the same serial link, just as Ethernet supports multiple network types over the same LAN. PPP replaces the earlier Serial Line Internet Protocol (SLIP) that only supports IP over a serial link. PPTP is a tunneling protocol.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 3: TCP/IP from a Security Viewpoint.

NEW QUESTION: 346
Which of the following ports does NOT normally need to be open for a mail server to operate?
A. Port 110
B. Port 25
C. Port 119
D. Port 143
Answer: C (LEAVE A REPLY)
Port 119 is normally used for the Network News Transfer Protocol. It is thus not need for a mail server, which would normally listen to ports 25 (SMTP), 110 (POP3) and 143 (IMAP).
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 1: Understanding Firewalls.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest**

BraindumpsPass.com SSCP dumps with Test Engine here:
https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps,
40%OFF Special Discount: Exam-Tests)

NEW QUESTION: 347
What is called an exception to the search warrant requirement that allows an officer to conduct a search without having the warrant in-hand if probable cause is present and destruction of the evidence is deemed imminent?
A. Evidence Circumstance Doctrine
B. Exigent Circumstance Doctrine
C. Evidence of Admissibility Doctrine
D. Exigent Probable Doctrine
Answer: (SHOW ANSWER)
An Exigent Circumstance is an unusual and time-sensitive circumstance that justifies conduct that might not be permissible or lawful in other circumstances.
For example, exigent circumstances may justify actions by law enforcement officers acting without a warrant such as a mortal danger to a young child. Examples of other exigent circumstances include protecting evidence or property from imminent destruction.
In US v Martinez, Justice Thomas of the United States Court of Appeal used these words:
"As a general rule, we define exigent circumstances as those circumstances that would cause a reasonable person to believe that entry was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."
In Alvarado, Justice Blackburn of the Court of Appeals of Georgia referred to exigent circumstances in the context of a drug bust:
"The exigent circumstance doctrine provides that when probable cause has been established to believe that evidence will be removed or destroyed before a warrant can be obtained, a warrantless search and seizure can be justified. As many courts have noted, the need for the exigent circumstance doctrine is particularly compelling in narcotics cases, because contraband and records can be easily and quickly destroyed while a search is progressing. Police officers relying on this exception must demonstrate an objectively reasonable basis for deciding that immediate action is required."
All of the other answers were only detractors made up and not legal terms.
Reference(s) used for this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 313. and
http://www.duhaime.org/LegalDictionary/E/ExigentCircumstances.aspx

NEW QUESTION: 348
All of the following can be considered essential business functions that should be identified when creating a Business Impact Analysis (BIA) except one. Which of the following would not be considered an essential element of the BIA but an important TOPIC to include within the BCP plan:

A. IT Network Support
B. Accounting
C. Public Relations
D. Purchasing
Answer: C (LEAVE A REPLY)
Public Relations, although important to a company, is not listed as an essential business function that should be identified and have loss criteria developed for. All other entries are considered essential and should be identified and have loss criteria developed.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 598).

NEW QUESTION: 349
When referring to a computer crime investigation, which of the following would be the MOST important step required in order to preserve and maintain a proper chain of custody of evidence:
A. Evidence has to be collected in accordance with all laws and all legal regulations.
B. Law enforcement officials should be contacted for advice on how and when to collect critical information.
C. Verifiable documentation indicating the who, what, when, where, and how the evidence was handled should be available.
D. Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Two concepts that are at the heart of dealing effectively with digital/electronic evidence, or any evidence for that matter, are the chain of custody and authenticity/integrity.
The chain of custody refers to the who, what, when, where, and how the evidence was handled-from its identification through its entire life cycle, which ends with destruction or permanent archiving.
Any break in this chain can cast doubt on the integrity of the evidence and on the professionalism of those directly involved in either the investigation or the collection and handling of the evidence. The chain of custody requires following a formal process that is well documented and forms part of a standard operating procedure that is used in all cases, no exceptions.
The following are incorrect answers:
Evidence has to be collected in accordance with all laws and legal regulations. Evidence would have to be collected in accordance with applicable laws and regulations but not necessarily with ALL laws and regulations. Only laws and regulations that applies would be followed.
Law enforcement officials should be contacted for advice on how and when to collect critical information. It seems you failed to do your homework, once you have an incident it is a bit late to do this. Proper crime investigation as well as incident response is all about being prepared ahead of time. Obviously, you are improvising if you need to call law enforcement to find out what to do. It is a great way of contaminating

your evidence by mistake if you don't have a well documented processs with clear procedures that needs to be followed.
Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation. Specific legal requirements exists for log retention and they are not the same as normal business records. Laws such as Basel, HIPPAA, SOX, and others has specific requirements.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 23465-23470). Auerbach Publications. Kindle Edition.
and
ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 282-285).

NEW QUESTION: 350
Which of the following category of UTP cables is specified to be able to handle gigabit Ethernet (1 Gbps) according to the EIA/TIA-568-B standards?
A. Category 5e UTP
B. Category 2 UTP
C. Category 3 UTP
D. Category 1e UTP
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Categories 1 through 6 are based on the EIA/TIA-568-B standards.
On the newer wiring for LANs is CAT5e, an improved version of CAT5 which used to be outside of the standard, for more information on twisted pair, please see: twisted pair.
Category Cable Type Mhz Usage Speed
CAT1 UTP Analog voice, Plain Old Telephone System (POTS)
CAT2 UTP 4 Mbps on Token Ring, also used on Arcnet networks
CAT3 UTP, ScTP, STP 16 MHz 10 Mbps
CAT4 UTP, ScTP, STP 20 MHz 16 Mbps on Token Ring Networks
CAT5 UTP, ScTP, STP 100 MHz 100 Mbps on ethernet, 155 Mbps on ATM
CAT5e UTP, ScTP, STP 100 MHz 1 Gbps (out of standard version, improved version of CAT5) CAT6 UTP, ScTP, STP 250 MHz 10 Gbps CAT7 ScTP, STP 600 M 100 Gbps Category 6 has a minumum of 250 MHz of bandwidth. Allowing 10/100/1000 use with up to 100 meter cable length, along with 10GbE over shorter distances.
Category 6a or Augmented Category 6 has a minimum of 500 MHz of bandwidth. It is the newest standard and allows up to 10GbE with a length up to 100m.
Category 7 is a future cabling standard that should allow for up to 100GbE over 100 meters of cable. Expected availability is in 2013. It has not been approved as a cable standard, and anyone now selling you Cat. 7 cable is fooling you.

REFERENCES:
http://donutey.com/ethernet.php
http://en.wikipedia.org/wiki/TIA/EIA-568-B
http://en.wikipedia.org/wiki/Category_1_cable

NEW QUESTION: 351
Contracts and agreements are often times unenforceable or hard to enforce in which of the following alternate facility recovery agreement?
A. hot site
B. warm site
C. cold site
D. reciprocal agreement
Answer: D (LEAVE A REPLY)
A reciprocal agreement is where two or more organizations mutually agree to provide facilities to the other if a disaster occurs. The organizations must have similiar hardware and software configurations. Reciprocal agreements are often not legally binding. Reciprocal agreements are not contracts and cannot be enforced. You cannot force someone you have such an agreement with to provide processing to you.
Government regulators do not accept reciprocal agreements as valid disaster recovery sites.
Cold sites are empty computer rooms consisting only of environmental systems, such as air conditioning and raised floors, etc. They do not meet the requirements of most regulators and boards of directors that the disaster plan be tested at least annually.
Time Brokers promise to deliver processing time on other systems. They charge a fee, but cannot guaranty that processing will always be available, especially in areas that experienced multiple disasters.
With the exception of providing your own hot site, commercial hot sites provide the greatest protection. Most will allow you up to six weeks to restore your sites if you declare a disaster. They also permit an annual amount of time to test the Disaster Plan.
References:
OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369)
The following answers are incorrect:
hot site. Is incorrect because you have a contract in place stating what services are to be provided.
warm site. Is incorrect because you have a contract in place stating what services are to be provided.
cold site. Is incorrect because you have a contract in place stating what services are to be provided.

NEW QUESTION: 352
Which of the following statements pertaining to a Criticality Survey is incorrect?

A. It is implemented to gather input from all personnel that is going to be part of the recovery teams.
B. The purpose of the survey must be clearly stated.
C. Management's approval should be obtained before distributing the survey.
D. Its intent is to find out what services and systems are critical to keeping the organization in business.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The Criticality Survey is implemented through a standard questionnaire to gather input from the most knowledgeable people. Not all personnel that is going to be part of recovery teams is necessarily able to help in identifying critical functions of the organization.
The intent of such a survey is to identify the services and systems that are critical to the organization.
Having a clearly stated purpose for the survey helps in avoiding misinterpretations.
Management's approval of the survey should be obtained before distributing it.
Source: HARE, Chris, CISSP Study Guide: Business Continuity Planning Domain,

NEW QUESTION: 353
All of the following can be considered essential business functions that should be identified when creating a Business Impact Analysis (BIA) except one. Which of the following would not be considered an essential element of the BIA but an important TOPIC to include within the BCP plan:
A. IT Network Support
B. Accounting
C. Public Relations
D. Purchasing
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Public Relations, although important to a company, is not listed as an essential business function that should be identified and have loss criteria developed for.
All other entries are considered essential and should be identified and have loss criteria developed.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter
9: Disaster Recovery and Business continuity (page 598).

NEW QUESTION: 354
Which three things must be considered for the design, planning, and implementation of access control mechanisms? (Choose three)
A. Exposures
B. Objectives
C. Risks
D. Vulnerabilities
E. Threats
Answer: (SHOW ANSWER)

Threats, vulnerabilities, and risks are the three items that must be considered when designing access control mechanisms. Threats are possible violations, vulnerabilities are shortcomings in the system, and risks are measured by the likelihood that any particular threat may be carried out.

NEW QUESTION: 355
Buffer overflow and boundary condition errors are subsets of which of the following?
A. Race condition errors.
B. Access validation errors.
C. Exceptional condition handling errors.
D. Input validation errors.
Answer: (SHOW ANSWER)
Explanation/Reference:
In an input validation error, the input received by a system is not properly checked, resulting in a vulnerability that can be exploited by sending a certain input sequence. There are two important types of input validation errors: buffer overflows (input received is longer than expected input length) and boundary condition error (where an input received causes the system to exceed an assumed boundary). A race condition occurs when there is a delay between the time when a system checks to see if an operation is allowed by the security model and the time when the system actually performs the operation. In an access validation error, the system is vulnerable because the access control mechanism is faulty. In an exceptional condition handling error, the system somehow becomes vulnerable due to an exceptional condition that has arisen.
Source: DUPUIS, Clement, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 105).

NEW QUESTION: 356
Which of the following is the LEAST user accepted biometric device?
A. Fingerprint
B. Iris scan
C. Retina scan
D. Voice verification
Answer: C (LEAVE A REPLY)
Explanation/Reference:
The biometric device that is least user accepted is the retina scan, where a system scans the blood-vessel pattern on the backside of the eyeball. When using this device, an individual has to place their eye up to a device, and may require a puff of air to be blown into the eye. The iris scan only needs for an individual to glance at a camera that could be placed above a door.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter
4: Access Control (page 131).

NEW QUESTION: 357

Brute force attacks against encryption keys have increased in potency because of increased computing power. Which of the following is often considered a good protection against the brute force cryptography attack?

A. The use of good key generators.

B. The use of session keys.

C. Nothing can defend you against a brute force crypto key attack.

D. Algorithms that are immune to brute force key attacks.

Answer: (SHOW ANSWER)

If we assume a crytpo-system with a large key (and therefore a large key space) a brute force attack will likely take a good deal of time - anywhere from several hours to several years depending on a number of variables. If you use a session key for each message you encrypt, then the brute force attack provides the attacker with only the key for that one message. So, if you are encrypting 10 messages a day, each with a different session key, but it takes me a month to break each session key then I am fighting a loosing battle.

The other answers are not correct because:

"The use of good key generators" is not correct because a brute force key attack will eventually run through all possible combinations of key. Therefore, any key will eventually be broken in this manner given enough time.

"Nothing can defend you against a brute force crypto key attack" is incorrect, and not the best answer listed. While it is technically true that any key will eventually be broken by a brute force attack, the question remains "how long will it take?". In other words, if you encrypt something today but I can't read it for 10,000 years, will you still care? If the key is changed every session does it matter if it can be broken after the session has ended? Of the answers listed here, session keys are "often considered a good protection against the brute force cryptography attack" as the question asks.

"Algorithms that are immune to brute force key attacks" is incorrect because there currently are no such algorithms.

References:

Official ISC2 Guide page: 259

All in One Third Edition page: 623

NEW QUESTION: 358

In Mandatory Access Control, sensitivity labels attached to object contain what information?

A. The item's classification

B. The item's classification and category set

C. The item's category

D. The items's need to know

Answer: B (LEAVE A REPLY)

Explanation/Reference:

A Sensitivity label must contain at least one classification and one category set.

Category set and Compartment set are synonyms, they mean the same thing. The sensitivity label must contain at least one Classification and at least one Category. It is common in some environments for a single item to belong to multiple categories. The list of all the categories to which an item belongs is called a compartment set or category set.
The following answers are incorrect:
the item's classification. Is incorrect because you need a category set as well.
the item's category. Is incorrect because category set and classification would be both be required.
The item's need to know. Is incorrect because there is no such thing. The need to know is indicated by the catergories the object belongs to. This is NOT the best answer.
Reference(s) used for this question:
OIG CBK, Access Control (pages 186 - 188)
AIO, 3rd Edition, Access Control (pages 162 - 163)
AIO, 4th Edittion, Access Control, pp 212-214.
Wikipedia - http://en.wikipedia.org/wiki/Mandatory_Access_Control

NEW QUESTION: 359
Which of the following Kerberos components holds all users' and services' cryptographic keys?
A. The Key Distribution Service
B. The Authentication Service
C. The Key Distribution Center
D. The Key Granting Service
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The Key Distribution Center (KDC) holds all users' and services' cryptographic keys. It provides authentication services, as well as key distribution functionality. The Authentication Service is the part of the KDC that authenticates a principal. The Key Distribution Service and Key Granting Service are distracters and are not defined Kerberos components.
Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

NEW QUESTION: 360
Which of following is not a service provided by AAA servers (Radius, TACACS and DIAMETER)?
A. Authentication
B. Administration
C. Accounting
D. Authorization
Answer: B (LEAVE A REPLY)
Radius, TACACS and DIAMETER are classified as authentication,
authorization, and accounting (AAA) servers.
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management

Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.
also see:
The term "AAA" is often used, describing cornerstone concepts [of the AIC triad] Authentication, Authorization, and Accountability. Left out of the AAA acronym is Identification which is required before the three "A's" can follow. Identity is a claim, Authentication proves an identity, Authorization describes the action you can perform on a system once you have been identified and authenticated, and accountability holds users accountable for their actions.
Reference: CISSP Study Guide, Conrad Misenar, Feldman p. 10-11, (c) 2010 Elsevier.

NEW QUESTION: 361
How many bits of a MAC address uniquely identify a vendor, as provided by the IEEE?
A. 6 bits
B. 12 bits
C. 16 bits
D. 24 bits
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The MAC address is 48 bits long, 24 of which identify the vendor, as provided by the IEEE. The other 24 bits are provided by the vendor.
A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.
MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This is can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address. An example is many SOHO routers, where the ISP grants access to only one MAC address (used previously to inserting the router) so the router must use that MAC address on its Internet-facing NIC. Therefore the router administrator configures a MAC address to override the burned-in one.
A network node may have multiple NICs and each must have one unique MAC address per NIC.
See diagram below from Wikipedia showing the format of a MAC address. :
MAC Address format
Reference(s) used for this question:
http://en.wikipedia.org/wiki/MAC_address

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 362
When first analyzing an intrusion that has just been detected and confirming that it is a true positive, which of the following actions should be done as a first step if you wish to prosecute the attacker in court?
A. Back up the compromised systems.
B. Identify the attacks used to gain access.
C. Capture and record system information.
D. Isolate the compromised systems.
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
When an intrusion has been detected and confirmed, if you wish to prosecute the attacker in court, the following actions should be performed in the following order:
Capture and record system information and evidence that may be lost, modified, or not captured during the execution of a backup procedure. Start with the most volative memory areas first.
Make at least two full backups of the compromised systems, using hardware-write-protectable or write-once media. A first backup may be used to re-install the compromised system for further analysis and the second one should be preserved in a secure location to preserve the chain of custody of evidence.
Isolate the compromised systems.
Search for signs of intrusions on other systems.
Examine logs in order to gather more information and better identify other systems to which the intruder might have gained access.
Search through logs of compromised systems for information that would reveal the kind of attacks used to gain access.
Identify what the intruder did, for example by analyzing various log files, comparing checksums of known, trusted files to those on the compromised machine and by using other intrusion analysis tools.
Regardless of the exact steps being followed, if you wish to prosecute in a court of law it means you MUST capture the evidence as a first step before it could be lost or contaminated. You always start with the most volatile evidence first.
NOTE:
I have received feedback saying that some other steps may be done such as Disconnecting the system from the network or shutting down the system. This is true. However, those are not choices listed within the 4 choices attached to this question, you MUST avoid changing the question. You must stick to the four choices presented and pick which one is the best out of the four presented.

In real life, Forensic is not always black or white. There are many shades of grey. In real life you would have to consult your system policy (if you have one), get your Computer Incident team involved, and talk to your forensic expert and then decide what is the best course of action.
Reference(s) Used for this question:
http://www.newyorkcomputerforensics.com/learn/forensics_process.php
and
ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter
7: Responding to Intrusions (pages 273-277).

NEW QUESTION: 363
Which one of the following is usually not a benefit resulting from the use of firewalls?
A. reduces the risks of external threats from malicious hackers.
B. prevents the spread of viruses.
C. reduces the threat level on internal system.
D. allows centralized management and control of services.
Answer: (SHOW ANSWER)
Explanation/Reference:
This is not a benefit of a firewall. Most firewalls are limited when it comes to preventing the spread of viruses.
This question is testing your knowledge of Malware and Firewalls. The keywords within the questions are "usually" and "virus". Once again to come up with the correct answer, you must stay within the context of the question and really ask yourself which of the 4 choices is NOT usually done by a firewall.
Some of the latest Appliances such as Unified Threat Management (UTM) devices does have the ability to do virus scanning but most first and second generation firewalls would not have such ability.
Remember, the questions is not asking about all possible scenarios that could exist but only about which of the 4 choices presented is the BEST.
For the exam you must know your general classes of Malware. There are generally four major classes of malicious code that fall under the general definition of malware:
1. Virus: Parasitic code that requires human action or insertion, or which attaches itself to another program to facilitate replication and distribution. Virus-infected containers can range from e-mail, documents, and data file macros to boot sectors, partitions, and memory fobs. Viruses were the first iteration of malware and were typically transferred by floppy disks (also known as "sneakernet") and injected into memory when the disk was accessed or infected files were transferred from system to system.
2. Worm: Self-propagating code that exploits system or application vulnerabilities to replicate. Once on a system, it may execute embedded routines to alter, destroy, or monitor the system on which it is running, then move on to the next system. A worm is effectively a virus that does not require human interaction or other programs to infect systems.
3. Trojan Horse: Named after the Trojan horse of Greek mythology (and serving a very similar function), a Trojan horse is a general term referring to programs that appear desirable, but actually contain something

harmful. A Trojan horse purports to do one thing that the user wants while secretly performing other potentially malicious actions. For example, a user may download a game file, install it, and begin playing the game. Unbeknownst to the user, the application may also install a virus, launch a worm, or install a utility allowing an attacker to gain unauthorized access to the system remotely, all without the user's knowledge.
4. Spyware: Prior to its use in malicious activity, spyware was typically a hidden application injected through poor browser security by companies seeking to gain more information about a user's Internet activity. Today, those methods are used to deploy other malware, collect private data, send advertising or commercial messages to a system, or monitor system input, such as keystrokes or mouse clicks.
The following answers are incorrect:
reduces the risks of external threats from malicious hackers. This is incorrect because a firewall can reduce the risks of external threats from malicious hackers.
reduces the threat level on internal system. This is incorrect because a firewall can reduce the threat level on internal system.
allows centralized management and control of services. This is incorrect because a firewall can allow centralize management and control of services.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3989-4009). Auerbach Publications. Kindle Edition.

NEW QUESTION: 364
How often should tests and disaster recovery drills be performed?
A. At least once a quarter
B. At least once every 6 months
C. At least once a year
D. At least once every 2 years
Answer: (SHOW ANSWER)
Explanation/Reference:
Tests and disaster recovery drills should be performed at least once a year. The company should have no confidence in an untested plan. Since systems and processes can change, frequent testing will aid in ensuring a plan will succeed.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter
9: Disaster Recovery and Business continuity (page 621).

NEW QUESTION: 365
Under United States law, an investigator's notebook may be used in court in which of the following scenarios?
A. When the investigator is unwilling to testify.
B. When other forms of physical evidence are not available.
C. To refresh the investigators memory while testifying.

D. If the defense has no objections.

Answer: (SHOW ANSWER)

An investigator's notebook cannot be used as evidence is court. It can only be used by the investigator to refresh his memory during a proceeding, but cannot be submitted as evidence in any form.

The following answers are incorrect:

When the investigator is unwilling to testify. Is incorrect because the notebook cannot be submitted as evidence in any form.

When other forms of physical evidence are not available. Is incorrect because the notebook cannot be submitted as evidence in any form.

If the defense has no objections. Is incorrect because the notebook cannot be submitted as evidence in any form.

NEW QUESTION: 366

Which of the following is needed for System Accountability?

A. Audit mechanisms.

B. Documented design as laid out in the Common Criteria.

C. Authorization.

D. Formal verification of system design.

Answer: (SHOW ANSWER)

Section: Access Control

Explanation/Reference:

Is a means of being able to track user actions. Through the use of audit logs and other tools the user actions are recorded and can be used at a later date to verify what actions were performed.

Accountability is the ability to identify users and to be able to track user actions.

The following answers are incorrect:

Documented design as laid out in the Common Criteria. Is incorrect because the Common Criteria is an international standard to evaluate trust and would not be a factor in System Accountability.

Authorization. Is incorrect because Authorization is granting access to subjects, just because you have authorization does not hold the subject accountable for their actions.

Formal verification of system design. Is incorrect because all you have done is to verify the system design and have not taken any steps toward system accountability.

References:

OIG CBK Glossary (page 778)

NEW QUESTION: 367

An alternative to using passwords for authentication in logical or technical access control is:

A. manage without passwords

B. biometrics

C. not there

D. use of them for physical access control

Answer: B (LEAVE A REPLY)

Section: Access Control
Explanation/Reference:
An alternative to using passwords for authentication in logical or technical access control is biometrics. Biometrics are based on the Type 3 authentication mechanism-something you are.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION: 368
Which xDSL flavour can deliver up to 52 Mbps downstream over a single copper twisted pair?
A. VDSL
B. SDSL
C. HDSL
D. ADSL
Answer: A (LEAVE A REPLY)
Very-high data-rate Digital Subscriber Line (VDSL) can deliver up to 52 Mbps downstream over a single copper twisted pair over a relatively short distance (1000 to 4500 feet). DSL (Digital Subscriber Line) is a modem technology for broadband data access over ordinary copper telephone lines (POTS) from homes and businesses. xDSL refers collectively to all types of DSL, such as ADSL (and G.Lite), HDSL, SDSL, IDSL and VDSL etc. They are sometimes referred to as last-mile (or first mile) technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.
xDSL is similar to ISDN in as much as both operate over existing copper telephone lines (POTS) using sophisticated modulation schemes and both require the short runs to a central telephone office
Graphic below from: http://computer.howstuffworks.com/vdsl3.htm
DSL speed chart
The following are incorrect answers:
Single-line Digital Subscriber Line (SDSL) deliver 2.3 Mbps of bandwidth each way. High-rate Digital Subscriber Line (HDSL) deliver 1.544 Mbps of bandwidth each way. ADSL delivers a maximum of 8 Mbps downstream for a total combined speed of almost 9 Mbps up and down.
Reference used for this question:
http://computer.howstuffworks.com/vdsl3.htm and http://www.javvin.com/protocolxDSL.html and KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 115).

NEW QUESTION: 369
What attack involves the perpetrator sending spoofed packet(s) wich contains the same destination and source IP address as the remote host, the same port for the source and destination, having the SYN flag, and targeting any open ports that are open on the remote host?
A. Boink attack
B. Land attack
C. Teardrop attack

D. Smurf attack

Answer: B (LEAVE A REPLY)

Section: Network and Telecommunications

Explanation/Reference:

The Land attack involves the perpetrator sending spoofed packet(s) with the SYN flag set to the victim's machine on any open port that is listening. The packet(s) contain the same destination and source IP address as the host, causing the victim's machine to reply to itself repeatedly. In addition, most systems experience a total freeze up, where as CTRL-ALT-DELETE fails to work, the mouse and keyboard become non operational and the only method of correction is to reboot via a reset button on the system or by turning the machine off.

The Boink attack, a modified version of the original Teardrop and Bonk exploit programs, is very similar to the Bonk attack, in that it involves the perpetrator sending corrupt UDP packets to the host. It however allows the attacker to attack multiple ports where Bonk was mainly directed to port 53 (DNS).

The Teardrop attack involves the perpetrator sending overlapping packets to the victim, when their machine attempts to re-construct the packets the victim's machine hangs.

A Smurf attack is a network-level attack against hosts where a perpetrator sends a large amount of ICMP echo (ping) traffic at broadcast addresses, all of it having a spoofed source address of a victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply each, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, there could potentially be hundreds of machines to reply to each packet.

Resources:

http://en.wikipedia.org/wiki/Denial-of-service_attack

http://en.wikipedia.org/wiki/LAND

NEW QUESTION: 370

Which of the following is NOT a true statement regarding the implementaton of the 3DES modes?

A. DES-EEE1 uses one key

B. DES-EEE2 uses two keys

C. DES-EEE3 uses three keys

D. DES-EDE2 uses two keys

Answer: A (LEAVE A REPLY)

Explanation/Reference:

There is no DES mode call DES-EEE1. It does not exist.

The following are the correct modes for triple-DES (3DES):

DES-EEE3 uses three keys for encryption and the data is encrypted, encrypted, encrypted; DES-EDE3 uses three keys and encrypts, decrypts and encrypts data.

DES-EEE2 and DES-EDE2 are the same as the previous modes, but the first and third operations use the same key.

Reference(s) used for this question:

Shon Harris, CISSP All In One (AIO) book, 6th edition , page 808

and
Official ISC2 Guide to the CISSP CBK, 2nd Edition (2010) , page 344-345

NEW QUESTION: 371
In the context of Biometric authentication, what is a quick way to compare the accuracy of devices. In general, the device that have the lowest value would be the most accurate. Which of the following would be used to compare accuracy of devices?
A. the CER is used.
B. the FRR is used
C. the FAR is used
D. the FER is used
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
equal error rate or crossover error rate (EER or CER): the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.
In the context of Biometric Authentication almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher False Reject Rate (FRR).
Conversely, if the sensitivity is decreased, the False Acceptance Rate (FAR) will increase.
Thus, to have a valid measure of the system performance, the CrossOver Error Rate (CER) is used.
The following are used as performance metrics for biometric systems:
false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, then he is treated as genuine that increase the FAR and hence performance also depends upon the selection of threshold value.
false reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
template capacity: the maximum number of sets of data which can be stored in the system.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

and
Wikipedia at: https://en.wikipedia.org/wiki/Biometrics

NEW QUESTION: 372
Which of the following types of Intrusion Detection Systems uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host?
A. Network-based ID systems.
B. Anomaly Detection.
C. Host-based ID systems.
D. Signature Analysis.
Answer: B (LEAVE A REPLY)
There are two basic IDS analysis methods: pattern matching (also called signature analysis) and anomaly detection.
Anomaly detection uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host. Anomalies may include but are not limited to:
Multiple failed log-on attempts Users logging in at strange hours Unexplained changes to system clocks Unusual error messages
The following are incorrect answers: Network-based ID Systems (NIDS) are usually incorporated into the network in a passive architecture, taking advantage of promiscuous mode access to the network. This means that it has visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network or the systems and applications utilizing the network.
Host-based ID Systems (HIDS) is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network. This offers unfettered access to system logs, processes, system information, and device information, and virtually eliminates limits associated with encryption. The level of integration represented by HIDS increases the level of visibility and control at the disposal of the HIDS application.
Signature Analysis Some of the first IDS products used signature analysis as their detection method and simply looked for known characteristics of an attack (such as specific packet sequences or text in the data stream) to produce an alert if that pattern was detected. For example, an attacker manipulating an FTP server may use a tool that sends a specially constructed packet. If that particular packet pattern is known, it can be represented in the form of a signature that IDS can then compare to incoming packets. Pattern-based IDS will have a database of hundreds, if not thousands, of signatures that are compared to traffic streams. As new attack signatures are produced, the system is updated, much like antivirus solutions. There are drawbacks to pattern-based IDS. Most importantly, signatures can only exist for known attacks. If a new or different attack vector is used, it will not match a known signature and, thus, slip past the IDS. Additionally, if an attacker knows that the IDS is present, he or she can alter his or her

methods to avoid detection. Changing packets and data streams, even slightly, from known signatures can cause an IDS to miss the attack. As with some antivirus systems, the IDS is only as good as the latest signature database on the system.
For additional information on Intrusion Detection Systems
http://en.wikipedia.org/wiki/Intrusion_detection_system
Reference(s) used for this question: Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3623-3625, 3649-3654, 3666-3686). Auerbach Publications. Kindle Edition.

NEW QUESTION: 373
Memory management in TCSEC levels B3 and A1 operating systems may utilize "data hiding". What does this mean?
A. System functions are layered, and none of the functions in a given layer can access data outside that layer.
B. Auditing processes and their memory addresses cannot be accessed by user processes.
C. Only security processes are allowed to write to ring zero memory.
D. It is a form of strong encryption cipher.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Data Hiding is protecting data so that it is only available to higher levels this is done and is also performed by layering, when the software in each layer maintains its own global data and does not directly reference data outside its layers.
The following answers are incorrect:
Auditing processes and their memory addresses cannot be accessed by user processes. Is incorrect because this does not offer data hiding.
Only security processes are allowed to write to ring zero memory. This is incorrect, the security kernel would be responsible for this.
It is a form of strong encryption cipher. Is incorrect because this does not conform to the definition of data hiding.

NEW QUESTION: 374
Which of the following best describes what would be expected at a "hot site"?
A. Computers, climate control, cables and peripherals
B. Computers and peripherals
C. Computers and dedicated climate control systems.
D. Dedicated climate control systems
Answer: A (LEAVE A REPLY)
A Hot Site contains everything needed to become operational in the shortest amount of time.
The following answers are incorrect:
Computers and peripherals. Is incorrect because no mention is made of cables. You would not be fully operational without those.

Computers and dedicated climate control systems. Is incorrect because no mention is made of peripherals. You would not be fully operational without those.
Dedicated climate control systems. Is incorrect because no mentionis made of computers, cables and peripherals. You would not be fully operational without those.
According to the OIG, a hot site is defined as a fully configured site with complete customer required hardware and software provided by the service provider. A hot site in the context of the CBK is always a RENTAL place. If you have your own site fully equipped that you make use of in case of disaster that would be called a redundant site or an alternate site.
Wikipedia: "A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data."
References:
OIG CBK, Business Continuity and Disaster Recovery Planning (pages 367 - 368)
AIO, 3rd Edition, Business Continuity Planning (pages 709 - 714)
AIO, 4th Edition, Business Continuity Planning , p 790.
Wikipedia - http://en.wikipedia.org/wiki/Hot_site#Hot_Sites

NEW QUESTION: 375
Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?
A. B
B. A
C. C
D. D
Answer: A (LEAVE A REPLY)
Explanation/Reference:
B level is the first Mandatory Access Control Level.
First published in 1983 and updated in 1985, the TCSEC, frequently referred to as the Orange Book, was a United States Government Department of Defense (DoD) standard that sets basic standards for the implementation of security protections in computing systems. Primarily intended to help the DoD find products that met those basic standards, TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information on military and government systems. As such, it was strongly focused on enforcing confidentiality with no focus on other aspects of security such as integrity or availability. Although it has since been superseded by the common criteria, it influenced the development of other product evaluation criteria, and some of its basic approach and terminology continues to be used.
Reference used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17920-17926). Auerbach Publications. Kindle Edition.
and
THE source for all TCSEC "level" questions: http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt (paragraph 3 for this one)

NEW QUESTION: 376
Each data packet is assigned the IP address of the sender and the IP address of the:
A. recipient.
B. host.
C. node.
D. network.
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Each data packet is assigned the IP address of the sender and the IP address of the recipient. The term network refers to the part of the IP address that identifies each network. The terms host and node refer to the parts of the IP address that identify a specific machine on a network.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 377
Secure Shell (SSH-2) provides all the following services except:
A. secure remote login
B. command execution
C. port forwarding
D. user authentication
Answer: D (LEAVE A REPLY)
This is one of the tricky negative question. You have to pay close attention to the word EXCEPT within the question.
The SSH transport layer is a secure, low level transport protocol. It provides strong encryption, cryptographic host authentication, and integrity protection.
Authentication in this protocol level is host-based; this protocol does not perform user authentication. A higher level protocol for user authentication can be designed on top of this protocol.
The protocol has been designed to be simple and flexible to allow parameter negotiation, and to minimize the number of round-trips. The key exchange method, public key

algorithm, symmetric encryption algorithm, message authentication algorithm, and hash algorithm are all negotiated. It is expected that in most environments, only 2 round-trips will be needed for full key exchange, server authentication, service request, and acceptance notification of service request. The worst case is 3 round-trips.
The following are incorrect answers:
"Remote log-on" is incorrect. SSH does provide remote log-on.
"Command execution" is incorrect. SSH does provide command execution.
"Port forwarding" is incorrect. SSH does provide port forwarding. SSH also has a wonderful feature called SSH Port Forwarding, sometimes called SSH Tunneling, which allows you to establish a secure SSH session and then tunnel arbitrary TCP connections through it. Tunnels can be created at any time, with almost no effort and no programming, which makes them very appealing. See the article below in the reference to take a look at SSH Port Forwarding in detail, as it is a very useful but often misunderstood technology. SSH Port Forwarding can be used for secure communications in a myriad of different ways.
You can see a nice tutorial on the PUTTY web site on how to use PUTTY to do port forwarding at:
http://www.cs.uu.nl/technical/services/ssh/putty/puttyfw.html
Reference(s) used for this question:
RFC 4253 at https://www.ietf.org/rfc/rfc4253.txt
and
SSH Port Forwarding by Symantec

NEW QUESTION: 378
An application layer firewall is also called a:
A. Proxy
B. A Presentation Layer Gateway.
C. A Session Layer Gateway.
D. A Transport Layer Gateway.
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
An application layer firewall can also be called a proxy.
"A presentation layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.
"A session layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.
"A transport layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.

References:
CBK, p. 467
AIO3, pp. 486 - 490, 960

NEW QUESTION: 379
Which backup method copies only files that have changed since the last full backup, but does not clear the archive bit?
A. Differential backup method.
B. Full backup method.
C. Incremental backup method.
D. Tape backup method.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
One of the key item to understand regarding backup is the archive bit. The archive bit is used to determine what files have been backuped already. The archive bit is set if a file is modified or a new file is created, this indicates to the backup program that it has to be saved on the next backup. When a full backup is performed the archive bit will be cleared indicating that the files were backup. This allows backup programs to do an incremental or differential backup that only backs up the changes to the filesystem since the last time the bit was cleared
Full Backup (or Reference Backup)
A Full backup will backup all the files and folders on the drive every time you run the full backup. The archive bit is cleared on all files indicating they were all backuped.
Advantages:
All files from the selected drives and folders are backed up to one backup set.
In the event you need to restore files, they are easily restored from the single backup set.
Disadvantages:
A full backup is more time consuming than other backup options.
Full backups require more disk, tape, or network drive space.
Incremental Backup
An incremental backup provides a backup of files that have changed or are new since the last incremental backup.
For the first incremental backup, all files in the file set are backed up (just as in a full backup). If you use the same file set to perform a incremental backup later, only the files that have changed are backed up. If you use the same file set for a third backup, only the files that have changed since the second backup are backed up, and so on.
Incremental backup will clear the archive bit.
Advantages:
Backup time is faster than full backups.
Incremental backups require less disk, tape, or network drive space.
You can keep several versions of the same files on different backup sets.
Disadvantages:

In order to restore all the files, you must have all of the incremental backups available.
It may take longer to restore a specific file since you must search more than one backup set to find the latest version of a file.
Differential Backup
A differential backup provides a backup of files that have changed since a full backup was performed. A differential backup typically saves only the files that are different or new since the last full backup.
Together, a full backup and a differential backup include all the files on your computer, changed and unchanged.
Differential backup do not clear the archive bits.
Advantages:
Differential backups require even less disk, tape, or network drive space than incremental backups.
Backup time is faster than full or incremental backups.
Disadvantages:
Restoring all your files may take considerably longer since you may have to restore both the last differential and full backup.
Restoring an individual file may take longer since you have to locate the file on either the differential or full backup.
For more info see: http://support.microsoft.com/kb/136621
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

NEW QUESTION: 380
Which of the following statements pertaining to Secure Sockets Layer (SSL) is false?
A. The SSL protocol was developed by Netscape to secure Internet client-server transactions.
B. The SSL protocol's primary use is to authenticate the client to the server using public key cryptography and digital certificates.
C. Web pages using the SSL protocol start with HTTPS
D. SSL can be used with applications such as Telnet, FTP and email protocols.
Answer: B (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
All of these statements pertaining to SSL are true except that it is primary use is to authenticate the client to the server using public key cryptography and digital certificates. It is the opposite, Its primary use is to authenticate the server to the client.
The following reference(s) were used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 170).

NEW QUESTION: 381
What is the RESULT of a hash algorithm being applied to a message ?
A. A digital signature

B. A ciphertext
C. A message digest
D. A plaintext
Answer: (SHOW ANSWER)
Explanation/Reference:
As when a hash algorithm is applied on a message , it produces a message digest.
The other answers are incorrect because :
A digital signature is a hash value that has been encrypted with a sender's private key.
A ciphertext is a message that appears to be unreadable.
A plaintext is a readable data.
Reference : Shon Harris , AIO v3 , Chapter-8 : Cryptography , Page : 593-594 , 640 , 648

NEW QUESTION: 382
Which of the following is NOT a form of detective administrative control?
A. Rotation of duties
B. Required vacations
C. Separation of duties
D. Security reviews and audits
Answer: C (LEAVE A REPLY)
Detective administrative controls warn of administrative control violations. Rotation of duties, required vacations and security reviews and audits are forms of detective administrative controls. Separation of duties is the practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process, thus a preventive control rather than a detective control.
Source: DUPUIS, Cl?ment, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0 (march 2002).

NEW QUESTION: 383
In biometrics, "one-to-many" search against database of stored biometric images is done in:
A. Authentication
B. Identification
C. Identities
D. Identity-based access control
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
In biometrics, identification is a "one-to-many" search of an individual's characteristics from a database of stored images.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

NEW QUESTION: 384

There are 5 classes of IP addresses available, but only 3 classes are in common use today, identify the three: (Choose three)
A. Class D: 224-255
B. Class E: 0.0.0.0 - 127.0.0.1
C. Class A: 1-126
D. Class B: 128-191
E. Class C: 192-223
Answer: C,D,E (LEAVE A REPLY)

NEW QUESTION: 385
Which of the following is NOT a symmetric key algorithm?
A. Blowfish
B. Digital Signature Standard (DSS)
C. Triple DES (3DES)
D. RC5
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Digital Signature Standard (DSS) specifies a Digital Signature Algorithm (DSA) appropriate for applications requiring a digital signature, providing the capability to generate signatures (with the use of a private key) and verify them (with the use of the corresponding public key).
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter
8: Cryptography (page 550).
Reference: DSS: http://www.itl.nist.gov/fipspubs/fip186.htm.

NEW QUESTION: 386
Which of the following statements is NOT true of IPSec Transport mode?
A. It is required for gateways providing access to internal systems
B. Set-up when end-point is host or communications terminates at end-points
C. If used in gateway-to-host communication, gateway must act as host
D. When ESP is used for the security protocol, the hash is only applied to the upper layer protocols contained in the packet
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

NEW QUESTION: 387
Which backup method only copies files that have been recently added or changed and also leaves the archive bit unchanged?

A. Full backup method
B. Incremental backup method
C. Fast backup method
D. Differential backup method
Answer: D (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
A differential backup is a partial backup that copies a selected file to tape only if the archive bit for that file is turned on, indicating that it has changed since the last full backup. A differential backup leaves the archive bits unchanged on the files it copies.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
69).
Also see: http://e-articles.info/e/a/title/Backup-Types/
Backup software can use or ignore the archive bit in determining which files to back up, and can either turn the archive bit off or leave it unchanged when the backup is complete. How the archive bit is used and manipulated determines what type of backup is done, as follows Full backup A full backup, which Microsoft calls a normal backup, backs up every selected file, regardless of the status of the archive bit. When the backup completes, the backup software turns off the archive bit for every file that was backed up. Note that "full" is a misnomer because a full backup backs up only the files you have selected, which may be as little as one directory or even a single file, so in that sense Microsoft's terminology is actually more accurate. Given the choice, full backup is the method to use because all files are on one tape, which makes it much easier to retrieve files from tape when necessary. Relative to partial backups, full backups also increase redundancy because all files are on all tapes. That means that if one tape fails, you may still be able to retrieve a given file from another tape.
Differential backup
A differential backup is a partial backup that copies a selected file to tape only if the archive bit for that file is turned on, indicating that it has changed since the last full backup. A differential backup leaves the archive bits unchanged on the files it copies. Accordingly, any differential backup set contains all files that have changed since the last full backup. A differential backup set run soon after a full backup will contain relatively few files.
One run soon before the next full backup is due will contain many files, including those contained on all previous differential backup sets since the last full backup. When you use differential backup, a complete backup set comprises only two tapes or tape sets: the tape that contains the last full backup and the tape that contains the most recent differential backup.
Incremental backup
An incremental backup is another form of partial backup. Like differential backups, Incremental Backups copy a selected file to tape only if the archive bit for that file is turned on. Unlike the differential backup, however, the incremental backup clears the archive bits for the files it backs up. An incremental backup set therefore contains only files that have changed since the last full backup or the last incremental

backup. If you run an incremental backup daily, files changed on Monday are on the Monday tape, files changed on Tuesday are on the Tuesday tape, and so forth. When you use an incremental backup scheme, a complete backup set comprises the tape that contains the last full backup and all of the tapes that contain every incremental backup done since the last normal backup. The only advantages of incremental backups are that they minimize backup time and keep multiple versions of files that change frequently. The disadvantages are that backed-up files are scattered across multiple tapes, making it difficult to locate any particular file you need to restore, and that there is no redundancy. That is, each file is stored only on one tape.
Full copy backup
A full copy backup (which Microsoft calls a copy backup) is identical to a full backup except for the last step.
The full backup finishes by turning off the archive bit on all files that have been backed up. The full copy backup instead leaves the archive bits unchanged. The full copy backup is useful only if you are using a combination of full backups and incremental or differential partial backups. The full copy backup allows you to make a duplicate "full" backup-e.g., for storage offsite, without altering the state of the hard drive you are backing up, which would destroy the integrity of the partial backup rotation.
Some Microsoft backup software provides a bizarre backup method Microsoft calls a daily copy backup. This method ignores the archive bit entirely and instead depends on the date- and timestamp of files to determine which files should be backed up. The problem is, it's quite possible for software to change a file without changing the date- and timestamp, or to change the date- and timestamp without changing the contents of the file. For this reason, we regard the daily copy backup as entirely unreliable and recommend you avoid using it.

NEW QUESTION: 388
What is the appropriate role of the security analyst in the application system development or acquisition project?
A. policeman
B. control evaluator & consultant
C. data owner
D. application user
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The correct answer is "control evaluator & consultant". During any system development or acquisition, the security staff should evaluate security controls and advise (or consult) on the strengths and weaknesses with those responsible for making the final decisions on the project.
The other answers are not correct because:
policeman - It is never a good idea for the security staff to be placed into this type of role (though it is sometimes unavoidable). During system development or acquisition, there should be no need of anyone filling the role of policeman.

data owner - In this case, the data owner would be the person asking for the new system to manage, control, and secure information they are responsible for. While it is possible the security staff could also be the data owner for such a project if they happen to have responsibility for the information, it is also possible someone else would fill this role. Therefore, the best answer remains "control evaluator & consultant".
application user - Again, it is possible this could be the security staff, but it could also be many other people or groups. So this is not the best answer.
Reference:
Official ISC2 Guide page: 555 - 560
All in One Third Edition page: 832 - 846

NEW QUESTION: 389
What can be defined as an event that could cause harm to the information systems?
A. A risk
B. A threat
C. A vulnerability
D. A weakness
Answer: (SHOW ANSWER)
Explanation/Reference:
A threat is an event or activity that has the potential to cause harm to the information systems. A risk is the probability that a threat will materialize. A vulnerability, or weakness, is a lack of a safeguard, which may be exploited by a threat, causing harm to the information systems.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 1: Access Control Systems (page 32).

NEW QUESTION: 390
What is malware that can spread itself over open network connections?
A. Worm
B. Rootkit
C. Adware
D. Logic Bomb
Answer: (SHOW ANSWER)
Explanation/Reference:
Computer worms are also known as Network Mobile Code, or a virus-like bit of code that can replicate itself over a network, infecting adjacent computers.
A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

A notable example is the SQL Slammer computer worm that spread globally in ten minutes on January 25,
2003. I myself came to work that day as a software tester and found all my SQL servers infected and actively trying to infect other computers on the test network.
A patch had been released a year prior by Microsoft and if systems were not patched and exposed to a 376 byte UDP packet from an infected host then system would become compromised.
Ordinarily, infected computers are not to be trusted and must be rebuilt from scratch but the vulnerability could be mitigated by replacing a single vulnerable dll called sqlsort.dll.
Replacing that with the patched version completely disabled the worm which really illustrates to us the importance of actively patching our systems against such network mobile code.
The following answers are incorrect:
- Rootkit: Sorry, this isn't correct because a rootkit isn't ordinarily classified as network mobile code like a worm is. This isn't to say that a rootkit couldn't be included in a worm, just that a rootkit isn't usually classified like a worm. A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.
- Adware: Incorrect answer. Sorry but adware isn't usually classified as a worm. Adware, or advertising-supported software, is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there. The term is sometimes used to refer to software that displays unwanted advertisements.
- Logic Bomb: Logic bombs like adware or rootkits could be spread by worms if they exploit the right service and gain root or admin access on a computer.
The following reference(s) was used to create this question:
The CCCure CompTIA Holistic Security+ Tutorial and CBT
and
http://en.wikipedia.org/wiki/Rootkit
and
http://en.wikipedia.org/wiki/Computer_worm
and
http://en.wikipedia.org/wiki/Adware

NEW QUESTION: 391
Which of the following is most concerned with personnel security?
A. Management controls
B. Operational controls
C. Technical controls

D. Human resources controls

Answer: B (LEAVE A REPLY)

Section: Security Operation Adimnistration

Explanation/Reference:

Many important issues in computer security involve human users, designers, implementers, and managers.

A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. Since operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems), personnel security is considered a form of operational control.

Operational controls are put in place to improve security of a particular system (or group of systems). They often require specialized expertise and often rely upon management activities as well as technical controls.

Implementing dual control and making sure that you have more than one person that can perform a task would fall into this category as well.

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access of misuse, facilitate detection of security violations, and support security requirements for applications and data.

Reference use for this question:

NIST SP 800-53 Revision 4 http://dx.doi.org/10.6028/NIST.SP.800-53r4

You can get it as a word document by clicking HERE

NIST SP 800-53 Revision 4 has superseded the document below:

SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Page A-18).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 392

Which of the following types of Intrusion Detection Systems uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host?

A. Network-based ID systems.

B. Anomaly Detection.
C. Host-based ID systems.
D. Signature Analysis.
Answer: B (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:
There are two basic IDS analysis methods: pattern matching (also called signature analysis) and anomaly detection.
Anomaly detection uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host. Anomalies may include but are not limited to:
Multiple failed log-on attempts
Users logging in at strange hours
Unexplained changes to system clocks
Unusual error messages
The following are incorrect answers:
Network-based ID Systems (NIDS) are usually incorporated into the network in a passive architecture, taking advantage of promiscuous mode access to the network. This means that it has visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network or the systems and applications utilizing the network.
Host-based ID Systems (HIDS) is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network. This offers unfettered access to system logs, processes, system information, and device information, and virtually eliminates limits associated with encryption. The level of integration represented by HIDS increases the level of visibility and control at the disposal of the HIDS application.
Signature Analysis Some of the first IDS products used signature analysis as their detection method and simply looked for known characteristics of an attack (such as specific packet sequences or text in the data stream) to produce an alert if that pattern was detected. For example, an attacker manipulating an FTP server may use a tool that sends a specially constructed packet. If that particular packet pattern is known, it can be represented in the form of a signature that IDS can then compare to incoming packets. Pattern-based IDS will have a database of hundreds, if not thousands, of signatures that are compared to traffic streams. As new attack signatures are produced, the system is updated, much like antivirus solutions. There are drawbacks to pattern-based IDS. Most importantly, signatures can only exist for known attacks. If a new or different attack vector is used, it will not match a known signature and, thus, slip past the IDS. Additionally, if an attacker knows that the IDS is present, he or she can alter his or her methods to avoid detection. Changing packets and data streams, even slightly, from known signatures can cause an IDS to miss the attack. As with some antivirus systems, the IDS is only as good as the latest signature database on the system.

For additional information on Intrusion Detection Systems - http://en.wikipedia.org/wiki/Intrusion_detection_system Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3623-3625, 3649-3654, 3666-3686). Auerbach Publications. Kindle Edition.

NEW QUESTION: 393
According to private sector data classification levels, how would salary levels and medical information be classified?
A. Public.
B. Internal Use Only.
C. Restricted.
D. Confidential.
Answer: (SHOW ANSWER)
Typically there are three to four levels of information classification used by most organizations:
Confidential: Information that, if released or disclosed outside of the organization, would create severe problems for the organization. For example, information that provides a competitive advantage is important to the technical or financial success (like trade secrets, intellectual property, or research designs), or protects the privacy of individuals would be considered confidential. Information may include payroll information, health records, credit information, formulas, technical designs, restricted regulatory information, senior management internal correspondence, or business strategies or plans. These may also be called top secret, privileged, personal, sensitive, or highly confidential. In other words this information is ok within a defined group in the company such as marketing or sales, but is not suited for release to anyone else in the company without permission.
The following answers are incorrect:
Public: Information that may be disclosed to the general public without concern for harming the company, employees, or business partners. No special protections are required, and information in this category is sometimes referred to as unclassified. For example, information that is posted to a company's public Internet site, publicly released announcements, marketing materials, cafeteria menus, and any internal documents that would not present harm to the company if they were disclosed would be classified as public. While there is little concern for confidentiality, integrity and availability should be considered.
Internal Use Only: Information that could be disclosed within the company, but could harm the company if disclosed externally. Information such as customer lists, vendor pricing, organizational policies, standards and procedures, and internal organization announcements would need baseline security protections, but do not rise to the level of protection as confidential information. In other words, the information may be used freely within the company but any unapproved use outside the company can pose a chance of harm.
Restricted: Information that requires the utmost protection or, if discovered by unauthorized personnel, would cause irreparable harm to the organization would have the highest level of classification. There may be very few pieces of information like this within an organization, but data classified at this level requires all the access control and protection

mechanisms available to the organization. Even when information classified at this level exists, there will be few copies of it
Reference(s) Used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 952-976). Auerbach Publications. Kindle Edition.

NEW QUESTION: 394
What would be considered the biggest drawback of Host-based Intrusion Detection systems (HIDS)?
A. It can be very invasive to the host operating system
B. Monitors all processes and activities on the host system only
C. Virtually eliminates limits associated with encryption
D. They have an increased level of visibility and control compared to NIDS
Answer: A (LEAVE A REPLY)
The biggest drawback of HIDS, and the reason many organizations resist its use, is that it can be very invasive to the host operating system. HIDS must have the capability to monitor all processes and activities on the host system and this can sometimes interfere with normal system processing.
HIDS versus NIDS A host-based IDS (HIDS) can be installed on individual workstations and/ or servers to watch for inappropriate or anomalous activity. HIDSs are usually used to make sure users do not delete system files, reconfigure important settings, or put the system at risk in any other way.
So, whereas the NIDS understands and monitors the network traffic, a HIDS's universe is limited to the computer itself. A HIDS does not understand or review network traffic, and a NIDS does not "look in" and monitor a system's activity. Each has its own job and stays out of the other's way.
The ISC2 official study book defines an IDS as:
An intrusion detection system (IDS) is a technology that alerts organizations to adverse or unwanted activity. An IDS can be implemented as part of a network device, such as a router, switch, or firewall, or it can be a dedicated IDS device monitoring traffic as it traverses the network. When used in this way, it is referred to as a network IDS, or NIDS. IDS can also be used on individual host systems to monitor and report on file, disk, and process activity on that host. When used in this way it is referred to as a host-based IDS, or HIDS.
An IDS is informative by nature and provides real-time information when suspicious activities are identified. It is primarily a detective device and, acting in this traditional role, is not used to directly prevent the suspected attack.
What about IPS?
In contrast, an intrusion prevention system (IPS), is a technology that monitors activity like an IDS but will automatically take proactive preventative action if it detects unacceptable activity. An IPS permits a predetermined set of functions and actions to occur on a network or system; anything that is not permitted is considered unwanted activity and blocked. IPS is engineered specifically to respond in real time to an event at the system or network layer. By proactively enforcing policy, IPS can thwart not only attackers, but also authorized users attempting to perform an action that is not within policy. Fundamentally, IPS is considered

an access control and policy enforcement technology, whereas IDS is considered network monitoring and audit technology.
The following answers were incorrect:
All of the other answer were advantages and not drawback of using HIDS
TIP FOR THE EXAM:
Be familiar with the differences that exists between an HIDS, NIDS, and IPS. Know that IDS's are mostly detective but IPS are preventive. IPS's are considered an access control and policy enforcement technology, whereas IDS's are considered network monitoring and audit technology.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5817-5822). McGraw-Hill. Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press), Domain1, Page 180-188 or on the kindle version look for Kindle Locations 3199-3203. Auerbach Publications.

NEW QUESTION: 395
The IP header contains a protocol field. If this field contains the value of 51, what type of data is contained within the ip datagram?
A. Transmission Control Protocol (TCP)
B. Authentication Header (AH)
C. User datagram protocol (UDP)
D. Internet Control Message Protocol (ICMP)
Answer: B (LEAVE A REPLY)
Explanation/Reference:
TCP has the value of 6
UDP has the value of 17
ICMP has the value of 1
Reference:
SANS http://www.sans.org/resources/tcpip.pdf?ref=3871

NEW QUESTION: 396
Which access model is most appropriate for companies with a high employee turnover?
A. Role-based access control
B. Mandatory access control
C. Lattice-based access control
D. Discretionary access control
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:

The underlying problem for a company with a lot of turnover is assuring that new employees are assigned the correct access permissions and that those permissions are removed when they leave the company. Selecting the best answer requires one to think about the access control options in the context of a company with a lot of flux in the employee population. RBAC simplifies the task of assigning permissions because the permissions are assigned to roles which do not change based on who belongs to them. As employees join the company, it is simply a matter of assigning them to the appropriate roles and their permissions derive from their assigned role. They will implicitely inherit the permissions of the role or roles they have been assigned to.
When they leave the company or change jobs, their role assignment is revoked/changed appropriately.
Mandatory access control is incorrect. While controlling access based on the clearence level of employees and the sensitivity of obects is a better choice than some of the other incorrect answers, it is not the best choice when RBAC is an option and you are looking for the best solution for a high number of employees constantly leaving or joining the company.
Lattice-based access control is incorrect. The lattice is really a mathematical concept that is used in formally modeling information flow (Bell-Lapadula, Biba, etc). In the context of the question, an abstract model of information flow is not an appropriate choice. CBK, pp. 324-325.
Discretionary access control is incorrect. When an employee joins or leaves the company, the object owner must grant or revoke access for that employee on all the objects they own. Problems would also arise when the owner of an object leaves the company. The complexity of assuring that the permissions are added and removed correctly makes this the least desirable solution in this situation.
References
Alll in One, third edition page 165
RBAC is discussed on pp. 189 through 191 of the ISC(2) guide.

NEW QUESTION: 397
In regards to information classification what is the main responsibility of information (data) owner?
A. determining the data sensitivity or classification level
B. running regular data backups
C. audit the data users
D. periodically check the validity and accuracy of the data
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Making the determination to decide what level of classification the information requires is the main responsibility of the data owner.
The data owner within classification is a person from Management who has been entrusted with a data set that belong to the company. It could be for example the Chief Financial Officer (CFO) who has been entrusted with all financial date or it could be the Human Resource Director who has been entrusted with all Human Resource data. The information owner will decide what classification will be applied to the data based on Confidentiality, Integrity, Availability, Criticality, and Sensitivity of the data.

The Custodian is the technical person who will implement the proper classification on objects in accordance with the Data Owner. The custodian DOES NOT decide what classification to apply, it is the Data Owner who will dictate to the Custodian what is the classification to apply.
NOTE:
The term Data Owner is also used within Discretionary Access Control (DAC). Within DAC it means the person who has created an object. For example, if I create a file on my system then I am the owner of the file and I can decide who else could get access to the file. It is left to my discretion. Within DAC access is granted based solely on the Identity of the subject, this is why sometimes DAC is referred to as Identity Based Access Control.
The other choices were not the best answer
Running regular backups is the responsibility of custodian.
Audit the data users is the responsibility of the auditors
Periodically check the validity and accuracy of the data is not one of the data owner responsibility
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 14, Chapter 1: Security Management Practices.

NEW QUESTION: 398
What would BEST define a covert channel?
A. An undocumented backdoor that has been left by a programmer in an operating system
B. An open system port that should be closed.
C. A communication channel that allows transfer of information in a manner that violates the system's security policy.
D. A trojan horse.
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
The Answer: A communication channel that allows transfer of information in a manner that violates the system's security policy.
A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way.
Receiving information in this manner clearly violates the system's security policy. The channel to transfer this unauthorized data is the result of one of the following conditions:* Oversight in the development of the product
* Improper implementation of access controls
* Existence of a shared resource between the two entities
* Installation of a Trojan horse
The following answers are incorrect:

An undocumented backdoor that has been left by a programmer in an operating system is incorrect because it is not a means by which unauthorized transfer of information takes place. Such backdoor is usually referred to as a Maintenance Hook.
An open system port that should be closed is incorrect as it does not define a covert channel.
A trojan horse is incorrect because it is a program that looks like a useful program but when you install it it would include a bonus such as a Worm, Backdoor, or some other malware without the installer knowing about it.
Reference(s) used for this question:
Shon Harris AIO v3 , Chapter-5 : Security Models & Architecture
AIOv4 Security Architecture and Design (pages 343 - 344)
AIOv5 Security Architecture and Design (pages 345 - 346)

NEW QUESTION: 399
What is called the probability that a threat to an information system will materialize?
A. Threat
B. Risk
C. Vulnerability
D. Hole
Answer: B (LEAVE A REPLY)
Risk: The potential for harm or loss to an information system or
network; the probability that a threat will materialize.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

NEW QUESTION: 400
A password audit consists of checking for _____?
A. Password aging
B. Password Strength
C. Minimum password length
D. All of the items listed
E. Blank Passwords
Answer: D (LEAVE A REPLY)

NEW QUESTION: 401
Which of the following would be the best reason for separating the test and development environments?
A. To restrict access to systems under test.
B. To control the stability of the test environment.
C. To segregate user and development staff.
D. To secure access to systems under development.
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration

Explanation/Reference:
The test environment must be controlled and stable in order to ensure that development projects are tested in a realistic environment which, as far as possible, mirrors the live environment.
Reference(s) used for this question:
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page
309).

NEW QUESTION: 402
Which of the following item would best help an organization to gain a common understanding of functions that are critical to its survival?
A. A risk assessment
B. A business assessment
C. A disaster recovery plan
D. A business impact analysis
Answer: D (LEAVE A REPLY)
A Business Impact Analysis (BIA) is an assessment of an organization's
business functions to develop an understanding of their criticality, recovery time objectives, and resources needed.
By going through a Business Impact Analysis, the organization will gain a common understanding of functions that are critical to its survival.
A risk assessment is an evaluation of the exposures present in an organization's external and internal environments.
A Business Assessment generally include Business Analysis as a discipline and it has heavy overlap with requirements analysis sometimes also called requirements engineering, but focuses on identifying the changes to an organization that are required for it to achieve strategic goals. These changes include changes to strategies, structures, policies, processes, and information systems.
A disaster recovery plan is the comprehensive statement of consistent actions to be taken before, during and after a disruptive event that causes a significant loss of information systems resources.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 57).

NEW QUESTION: 403
Which of the following choices describe a Challenge-response tokens generation?
A. A workstation or system that generates a random challenge string that the user enters into the token when prompted along with the proper PIN.
B. A workstation or system that generates a random login id that the user enters when prompted along with the proper PIN.

C. A special hardware device that is used to generate ramdom text in a cryptography system.
D. The authentication mechanism in the workstation or system does not determine if the owner should be authenticated.
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Challenge-response tokens are:
- A workstation or system generates a random challenge string and the owner enters the string into the token along with the proper PIN.
- The token generates a response that is then entered into the workstation or system.
- The authentication mechanism in the workstation or system then determines if the owner should be authenticated.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4:
Access Control (pages 136-137).

NEW QUESTION: 404
Which xDSL flavour, appropriate for home or small offices, delivers more bandwidth downstream than upstream and over longer distance?
A. VDSL
B. SDSL
C. ADSL
D. HDSL
Answer: C (LEAVE A REPLY)
Asymmetric digital subscriber line (ADSL) is designed to provide more bandwidth downstream (1 to 8 Mbps) than upstream (16 to 800Kb). DSL (Digital Subscriber Line) is a modem technology for broadband data access over ordinary copper telephone lines (POTS) from homes and businesses. xDSL refers collectively to all types of DSL, such as ADSL (and G.Lite), HDSL, SDSL, IDSL and VDSL etc. They are sometimes referred to as last-mile (or first mile) technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.
xDSL is similar to ISDN in as much as both operate over existing copper telephone lines (POTS) using sophisticated modulation schemes and both require the short runs to a central telephone office
Graphic below from: http://computer.howstuffworks.com/vdsl3.htm
DSL speed chart
The following are incorrect answers:
Single-line Digital Subscriber Line (SDSL) deliver 2.3 Mbps of bandwidth each way. High-rate Digital Subscriber Line (HDSL) deliver 1.544 Mbps of bandwidth each way.
Very-high data-rate Digital Subscriber Line (VDSL) can deliver up to 52 Mbps downstream over a single copper twisted pair over a relatively short distance (1000 to 4500 feet).

Reference used for this question:
http://computer.howstuffworks.com/vdsl3.htm and http://www.javvin.com/protocolxDSL.html and KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 115).

NEW QUESTION: 405
How long are IPv4 addresses?
A. 32 bits long.
B. 64 bits long.
C. 128 bits long.
D. 16 bits long.
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
IPv4 addresses are currently 32 bits long. IPv6 addresses are 128 bits long.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

NEW QUESTION: 406
This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and access than what is required for the tasks the user needs to fulfill. What best describes this scenario?
A. Excessive Rights
B. Excessive Access
C. Excessive Permissions
D. Excessive Privileges
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Even thou all 4 terms are very close to each other, the best choice is Excessive Privileges which would include the other three choices presented.
Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 645.
and

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here:

https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 407

_____ is the act of a user professing an identity to a system.

A. Validation

B. Authentication

C. Identification

D. Confirmation

Answer: C (LEAVE A REPLY)

Identification is used to establish user accountability. Many times identification takes the form of a logon ID.

NEW QUESTION: 408

Which of the following can be defined as the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors?

A. Unit testing

B. Pilot testing

C. Regression testing

D. Parallel testing

Answer: C (LEAVE A REPLY)

Section: Security Operation Adimnistration

Explanation

Explanation/Reference:

Regression testing is the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be the same as the data used in the original test. Unit testing refers to the testing of an individual program or module. Pilot testing is a preliminary test that focuses only on specific and predetermined aspects of a system. Parallel testing is the process of feeding test data into two systems and comparing the results.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).

NEW QUESTION: 409

If an organization were to monitor their employees' e-mail, it should not:

A. Monitor only a limited number of employees.

B. Inform all employees that e-mail is being monitored.

C. Explain who can read the e-mail and how long it is backed up.

D. Explain what is considered an acceptable use of the e-mail system.

Answer: (SHOW ANSWER)

Monitoring has to be conducted is a lawful manner and applied in a

consistent fashion; thus should be applied uniformly to all employees, not only to a small number.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 304).

NEW QUESTION: 410
A proxy is considered a:
A. first generation firewall.
B. third generation firewall.
C. second generation firewall.
D. fourth generation firewall.
Answer: C (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
The proxy (application layer firewall, circuit level proxy, or application proxy) is a second generation firewall
"First generation firewall" incorrect. A packet filtering firewall is a first generation firewall.
"Third generation firewall" is incorrect. Stateful Firewall are considered third generation firewalls
"Fourth generation firewall" is incorrect. Dynamic packet filtering firewalls are fourth generation firewalls
References:
CBK, p. 464
AIO3, pp. 482 - 484
Neither CBK or AIO3 use the generation terminology for firewall types but you will encounter it frequently as a practicing security professional. See http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/ scf4ch3.htm for a general discussion of the different generations.

NEW QUESTION: 411
Which of the following statements pertaining to the security kernel is incorrect?
A. The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept.
B. The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof.
C. The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner.
D. The security kernel is an access control concept, not an actual physical component.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
The reference monitor, not the security kernel is an access control concept.

The security kernel is made up of software, and firmware components that fall within the TCB and implements and enforces the reference monitor concept. The security kernel mediates all access and functions between subjects and objects. The security kernel is the core of the TCB and is the most commonly used approach to building trusted computing systems.
There are three main requirements of the security kernel:
* It must provide isolation for the processes carrying out the reference monitor concept, and the processes must be tamperproof.
* It must be invoked for every access attempt and must be impossible to circumvent. Thus, the security kernel must be implemented in a complete and foolproof way.
* It must be small enough to be able to be tested and verified in a complete and comprehensive manner.
The following answers are incorrect:
The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept. Is incorrect because this is the definition of the security kernel.
The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof. Is incorrect because this is one of the three requirements that make up the security kernel.
The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner. Is incorrect because this is one of the three requirements that make up the security kernel.

NEW QUESTION: 412
In addition to the accuracy of the biometric systems, there are other factors that must also be considered:
A. These factors include the enrollment time and the throughput rate, but not acceptability.
B. These factors do not include the enrollment time, the throughput rate, and acceptability.
C. These factors include the enrollment time, the throughput rate, and acceptability.
D. These factors include the enrollment time, but not the throughput rate, neither the acceptability.
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
In addition to the accuracy of the biometric systems, there are other factors that must also be considered. These factors include the enrollment time, the throughput rate, and acceptability.
Enrollment time is the time it takes to initially "register" with a system by providing samples of the biometric characteristic to be evaluated. An acceptable enrollment time is around two minutes.
For example, in fingerprint systems, the actual fingerprint is stored and requires approximately 250kb per finger for a high quality image. This level of information is required for one-to-many searches in forensics applications on very large databases.
In finger-scan technology, a full fingerprint is not stored-the features extracted from this fingerprint are stored using a small template that requires approximately 500 to 1000 bytes of storage. The original fingerprint cannot be reconstructed from this template.
Updates of the enrollment information may be required because some biometric characteristics, such as voice and signature, may change with time.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37 & 38.

NEW QUESTION: 413
What is the key size of the International Data Encryption Algorithm (IDEA)?
A. 64 bits
B. 128 bits
C. 160 bits
D. 192 bits
Answer: (SHOW ANSWER)
Explanation/Reference:
The International Data Encryption Algorithm (IDEA) is a block cipher that operates on 64 bit blocks of data with a 128-bit key. The data blocks are divided into 16 smaller blocks and each has eight rounds of mathematical functions performed on it. It is used in the PGP encryption software.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 3).

NEW QUESTION: 414
Which of the following protocols' primary function is to send messages between network devices regarding the health of the network?
A. Reverse Address Resolution Protocol (RARP).
B. Address Resolution Protocol (ARP).
C. Internet Protocol (IP).
D. Internet Control Message protocol (ICMP).
Answer: (SHOW ANSWER)
Explanation/Reference:
Its primary function is to send messages between network devices regarding the health of the network. ARP matches an IP address to an Ethernet address. RARP matches and Ethernet address to an IP address. ICMP runs on top of IP.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

NEW QUESTION: 415
The amount of risk remaining after security controls have been applied is referred to as:
A. Remaining risk
B. Residual risk
C. Acceptable risk
D. Outstanding risk
E. Enduring risk
Answer: B (LEAVE A REPLY)
Residual risk is the amount of risk remaining after security controls have been applied.

NEW QUESTION: 416
Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer 7 of the ISO/OSI Model?
A. Bridge
B. Repeater
C. Router
D. Gateway
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
A gateway is used to connect two networks using dissimilar protocols at the lower layers or it could also be at the highest level of the protocol stack.
Important Note:
For the purpose of the exam, you have to remember that a gateway is not synonymous to the term firewall.
The second thing you must remembers is the fact that a gateway act as a translation device.
It could be used to translate from IPX to TCP/IP for example. It could be used to convert different types of applications protocols and allow them to communicate together. A gateway could be at any of the OSI layers but usually tend to be higher up in the stack.
For your exam you should know the information below:
Repeaters
A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.
Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.
A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.
Repeater
Image Reference- http://www.erg.abdn.ac.uk/~gorry/course/images/repeater.gif Bridges A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network

segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge

Image Reference- http://www.oreillynet.com/network/2001/01/30/graphics/bridge.jpg Routers Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Router and Switch

Image Reference- http://www.computer-networking-success.com/images/router-switch.jpg Switches Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

Gateways

Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

Gateway Server

Image Reference-
http://static.howtoforge.com/images/screenshots/556af08d5e43aa768260f9e589dc547f-3024.jpg

The following answers are incorrect:

Repeater - A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

Bridges - A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Routers - Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to

their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary.
Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 263
Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 and 230

NEW QUESTION: 417
Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?
A. Steganography
B. Digital watermarking
C. Digital enveloping
D. Digital signature
Answer: (SHOW ANSWER)
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines digital watermarking as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data-text, graphics, images, video, or audio#and for detecting or extracting the marks later. The set of embedded bits (the digital watermark) is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. It is used as a measure to protect intellectual property rights. Steganography involves hiding the very existence of a message. A digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. A digital envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 418
Which of the following is not a preventive operational control?
A. Protecting laptops, personal computers and workstations.
B. Controlling software viruses.
C. Controlling data media access and disposal.
D. Conducting security awareness and technical training.
Answer: D (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:
Conducting security awareness and technical training to ensure that end users and system users are aware of the rules of behaviour and their responsibilities in protecting the organization's mission is an example of a preventive management control, therefore not an operational control.
Source: STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 37).

NEW QUESTION: 419
Which of the following is NOT a proper component of Media Viability Controls?
A. Storage
B. Writing
C. Handling
D. Marking
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Media Viability Controls include marking, handling and storage.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 231.

NEW QUESTION: 420
Which of the following items is NOT a benefit of cold sites?
A. No resource contention with other organisation
B. Quick Recovery
C. A secondary location is available to reconstruct the environment
D. Low Cost
Answer: B (LEAVE A REPLY)
Explanation/Reference:
A cold site is a permanent location that provide you with your own space that you can move into in case of a disaster or catastrophe. It is one of the cheapest solution available as a rental place but it is also the one that would take the most time to recover. A cold site usually takes one to two weeks for recoverey.
Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. The plan should include a trategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:
Dedicated site owned or operated by the organization. Also called redundant or alternate sites;
Reciprocal agreement or memorandum of agreement with an internal or external entity; and
Commercially leased facility.
Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types commonly categorized in terms of their operational readiness are cold sites, warm sites, or hot sites. Other variations or combinations of these can be found, but generally all variations retain similar core features found in one of these three site types.
Progressing from basic to advanced, the sites are described below:
Cold Sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.
ƒWarm Sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.

Hot Sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.
As discussed above, these three alternate site types are the most common. There are also variations, and hybrid mixtures of features from any one of the three. Each organization should evaluate its core requirements in order to establish the most effective solution.
Two examples of variations to the site types are:
ƒMobile Sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.
ƒMirrored Sites are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.
There are obvious cost and ready-time differences among the options. In these examples, the mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain, although they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours, but the time necessary for equipment installation and setup can increase this response time. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel and/or equipment there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same hazard as the organization's primary site.
The following reference(s) were used for this question:
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

NEW QUESTION: 421
Why is Network File System (NFS) used?
A. It enables two different types of file systems to interoperate.
B. It enables two different types of file systems to share Sun applications.
C. It enables two different types of file systems to use IP/IPX.
D. It enables two different types of file systems to emulate each other.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Network File System (NFS) is a TCP/IP client/server application developed by Sun that enables different types of file systems to interoperate regardless of operating system or network architecture.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 88.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here:

https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 422
Which of the following best corresponds to the type of memory addressing where the address location that is specified in the program instruction contains the address of the final desired location?
A. Direct addressing
B. Indirect addressing
C. Indexed addressing
D. Program addressing
Answer: (SHOW ANSWER)
Explanation/Reference:
Indirect addressing is when the address location that is specified in the program instruction contains the address of the final desired location. Direct addressing is when a portion of primary memory is accessed by specifying the actual address of the memory location. Indexed addressing is when the contents of the address defined in the program's instruction is added to that of an index register. Program addressing is not a defined memory addressing mode.
Source: WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 2).

NEW QUESTION: 423
What is the main concern with single sign-on?
A. Maximum unauthorized access would be possible if a password is disclosed.
B. The security administrator's workload would increase.
C. The users' password would be too hard to remember.
D. User access rights would be increased.
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
A major concern with Single Sign-On (SSO) is that if a user's ID and password are compromised, the intruder would have access to all the systems that the user was authorized for.
The following answers are incorrect:
The security administrator's workload would increase. Is incorrect because the security administrator's workload would decrease and not increase. The admin would not be responsible for maintaining multiple user accounts just the one.
The users' password would be too hard to remember. Is incorrect because the users would have less passwords to remember.
User access rights would be increased. Is incorrect because the user access rights would not be any different than if they had to log into systems manually.

NEW QUESTION: 424

What is called an attack in which an attacker floods a system with connection requests but does not respond when the target system replies to those requests?

A. Ping of death attack

B. SYN attack

C. Smurf attack

D. Buffer overflow attack

Answer: (SHOW ANSWER)

Explanation/Reference:

A SYN attack occurs when an attacker floods the target system's small "in-process" queue with connection requests, but it does not respond when the target system replies to those requests. This causes the target system to "time out" while waiting for the proper response, which makes the system crash or become unusable. A buffer overflow attack occurs when a process receives much more data than expected. One common buffer overflow attack is the ping of death, where an attacker sends IP packets that exceed the maximum legal length (65535 octets). A smurf attack is an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
76).

NEW QUESTION: 425

Which of the following phases of a software development life cycle normally addresses Due Care and Due Diligence?

A. Implementation

B. System feasibility

C. Product design

D. Software plans and requirements

Answer: D (LEAVE A REPLY)

Section: Security Operation Adimnistration

Explanation

Explanation/Reference:

The software plans and requirements phase addresses threats, vulnerabilities, security requirements, reasonable care, due diligence, legal liabilities, cost/benefit analysis, level of protection desired, test plans.

Implementation is incorrect because it deals with Installing security software, running the system, acceptance testing, security software testing, and complete documentation certification and accreditation (where necessary).

System Feasibility is incorrect because it deals with information security policy, standards, legal issues, and the early validation of concepts.

Product design is incorrect because it deals with incorporating security specifications, adjusting test plans and data, determining access controls, design documentation, evaluating encryption options, and verification.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter
7: Security Life Cycle Components, Figure 7.5 (page 346).

NEW QUESTION: 426
Which of the following is best defined as an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards?
A. Certification
B. Declaration
C. Audit
D. Accreditation
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Accreditation: is an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards. It is usually based on a technical certification of the system's security mechanisms.
Certification: Technical evaluation (usually made in support of an accreditation action) of an information system
\'s security features and other safeguards to establish the extent to which the system\'s design and implementation meet specified security requirements.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 427
Which of the following best allows risk management results to be used knowledgeably?
A. A vulnerability analysis
B. A likelihood assessment
C. An uncertainty analysis
D. A threat identification
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Risk management consists of two primary and one underlying activity; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one. After having performed risk

assessment and mitigation, an uncertainty analysis should be performed. Risk management must often rely on speculation, best guesses, incomplete data, and many unproven assumptions. A documented uncertainty analysis allows the risk management results to be used knowledgeably. A vulnerability analysis, likelihood assessment and threat identification are all parts of the collection and analysis of data part of the risk assessment, one of the primary activities of risk management.
Source: SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (pages 19-21).

NEW QUESTION: 428
Which of the following would be the MOST serious risk where a systems development life cycle methodology is inadequate?
A. The project will be completed late.
B. The project will exceed the cost estimates.
C. The project will be incompatible with existing systems.
D. The project will fail to meet business and user needs.
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
This is the most serious risk of inadequate systems development life cycle methodolgy.
The following answers are incorrect because :
The project will be completed late is incorrect as it is not most devastating as the above answer.
The project will exceed the cost estimates is also incorrect when compared to the above correct answer.
The project will be incompatible with existing systems is also incorrect when compared to the above correct answer.
Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 290).

NEW QUESTION: 429
Which of the following is related to physical security and is not considered a technical control?
A. Access control Mechanisms
B. Intrusion Detection Systems
C. Firewalls
D. Locks
Answer: D (LEAVE A REPLY)
Explanation/Reference:
All of the above are considered technical controls except for locks, which are physical controls.
Administrative, Technical, and Physical Security Controls
Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. For example, policy might

dictate (and procedures indicate how) that human resources conduct background checks on employees with access to sensitive information. Requiring that information be classified and the process to classify and review information classifications is another example of an administrative control. The organization security awareness program is an administrative control used to make employees cognizant of their security roles and responsibilities. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.
Technical security controls (also called logical controls) are devices, processes, protocols, and other measures used to protect the C.I.A. of sensitive information. Examples include logical access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems.
Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorized employees access to the data center do little good without some kind of physical access control.
From the GIAC.ORG website

NEW QUESTION: 430
Knowledge-based Intrusion Detection Systems (IDS) are more common than:
A. Network-based IDS
B. Host-based IDS
C. Behavior-based IDS
D. Application-Based IDS
Answer: (SHOW ANSWER)
Explanation/Reference:
Knowledge-based IDS are more common than behavior-based ID systems.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 63.
Application-Based IDS - "a subset of HIDS that analyze what's going on in an application using the transaction log files of the application." Source: Official ISC2 CISSP CBK Review Seminar Student Manual Version 7.0 p. 87
Host-Based IDS - "an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host." Source: Official ISC2 Guide to the CISSP CBK - p. 197
Network-Based IDS - "a network device, or dedicated system attached to the network, that monitors traffic traversing the network segment for which it is integrated." Source: Official ISC2 Guide to the CISSP CBK - p. 196

CISSP for dummies a book that we recommend for a quick overview of the 10 domains has nice and concise coverage of the subject:

Intrusion detection is defined as real-time monitoring and analysis of network activity and data for potential vulnerabilities and attacks in progress. One major limitation of current intrusion detection system (IDS) technologies is the requirement to filter false alarms lest the operator (system or security administrator) be overwhelmed with data. IDSes are classified in many different ways, including active and passive, network- based and host-based, and knowledge-based and behavior-based:

Active and passive IDS

An active IDS (now more commonly known as an intrusion prevention system - IPS) is a system that's configured to automatically block suspected attacks in progress without any intervention required by an operator. IPS has the advantage of providing real-time corrective action in response to an attack but has many disadvantages as well. An IPS must be placed in-line along a network boundary; thus, the IPS itself is susceptible to attack. Also, if false alarms and legitimate traffic haven't been properly identified and filtered, authorized users and applications may be improperly denied access. Finally, the IPS itself may be used to effect a Denial of Service (DoS) attack by intentionally flooding the system with alarms that cause it to block connections until no connections or bandwidth are available.

A passive IDS is a system that's configured only to monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. It isn't capable of performing any protective or corrective functions on its own. The major advantages of passive IDSes are that these systems can be easily and rapidly deployed and are not normally susceptible to attack themselves.

Network-based and host-based IDS

A network-based IDS usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

A host-based IDS requires small programs (or agents) to be installed on individual systems to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A host-based IDS can only monitor the individual host systems on which the agents are installed; it doesn't monitor the entire network.

Knowledge-based and behavior-based IDS

A knowledge-based (or signature-based) IDS references a database of previous attack profiles and known system vulnerabilities to identify active intrusion attempts. Knowledge-based IDS is currently more common than behavior-based IDS.

Advantages of knowledge-based systems include the following:

It has lower false alarm rates than behavior-based IDS.

Alarms are more standardized and more easily understood than behavior-based IDS.

Disadvantages of knowledge-based systems include these:

Signature database must be continually updated and maintained.

New, unique, or original attacks may not be detected or may be improperly classified.

A behavior-based (or statistical anomaly-based) IDS references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered.

Advantages of behavior-based systems include that they
Dynamically adapt to new, unique, or original attacks.
Are less dependent on identifying specific operating system vulnerabilities.
Disadvantages of behavior-based systems include
Higher false alarm rates than knowledge-based IDSes.
Usage patterns that may change often and may not be static enough to implement an effective behavior-based IDS.

NEW QUESTION: 431
Which of the following encryption methods is known to be unbreakable?
A. Symmetric ciphers.
B. DES codebooks.
C. One-time pads.
D. Elliptic Curve Cryptography.
Answer: (SHOW ANSWER)
Explanation/Reference:
A One-Time Pad uses a keystream string of bits that is generated completely at random that is used only once. Because it is used only once it is considered unbreakable.
The following answers are incorrect:
Symmetric ciphers. This is incorrect because a Symmetric Cipher is created by substitution and transposition. They can and have been broken
DES codebooks. This is incorrect because Data Encryption Standard (DES) has been broken, it was replaced by Advanced Encryption Standard (AES).
Elliptic Curve Cryptography. This is incorrect because Elliptic Curve Cryptography or ECC is typically used on wireless devices such as cellular phones that have small processors. Because of the lack of processing power the keys used at often small. The smaller the key, the easier it is considered to be breakable. Also, the technology has not been around long enough or tested thourough enough to be considered truly unbreakable.

NEW QUESTION: 432
The scope and focus of the Business continuity plan development depends most on:
A. Directives of Senior Management
B. Business Impact Analysis (BIA)
C. Scope and Plan Initiation
D. Skills of BCP committee
Answer: B (LEAVE A REPLY)
Explanation/Reference:
SearchStorage.com Definitions mentions "As part of a disaster recovery plan, BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on.

A BIA report quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance.
Where possible, impact is expressed monetarily for purposes of comparison. For example, a business may spend three times as much on marketing in the wake of a disaster to rebuild customer confidence."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 278.

NEW QUESTION: 433
The Secure Hash Algorithm (SHA-1) creates:
A. a fixed length message digest from a fixed length input message
B. a variable length message digest from a variable length input message
C. a fixed length message digest from a variable length input message
D. a variable length message digest from a fixed length input message
Answer: C (LEAVE A REPLY)
According to The CISSP Prep Guide, "The Secure Hash Algorithm (SHA-1) computes a fixed length message digest from a variable length input message." Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 160.
also see: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

NEW QUESTION: 434
Qualitative loss resulting from the business interruption does NOT usually include:
A. Loss of revenue
B. Loss of competitive advantage or market share
C. Loss of public confidence and credibility
D. Loss of market leadership
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
This question is testing your ability to evaluate whether items on the list are Qualitative or Quantitative. All of the items listed were Qualitative except Lost of Revenue which is Quantitative.
Those are mainly two approaches to risk analysis, see a description of each below:
A quantitative risk analysis is used to assign monetary and numeric values to all elements of the risk analysis process. Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks. It is more of a scientific or mathematical approach to risk analysis compared to qualitative.
A qualitative risk analysis uses a "softer" approach to the data elements of a risk analysis . It does not quantify that data, which means that it does not assign numeric values to the data so that they can be used in equations.

Qualitative and quantitative impact information should be gathered and then properly analyzed and interpreted.
The goal is to see exactly how a business will be affected by different threats.
The effects can be economical, operational, or both. Upon completion of the data analysis, it should be reviewed with the most knowledgeable people within the company to ensure that the findings are appropriate and that it describes the real risks and impacts the organization faces. This will help flush out any additional data points not originally obtained and will give a fuller understanding of all the possible business impacts.
Loss criteria must be applied to the individual threats that were identified. The criteria may include the following:
Loss in reputation and public confidence
Loss of competitive advantages
Increase in operational expenses
Violations of contract agreements
Violations of legal and regulatory requirements
Delayed income costs
Loss in revenue
Loss in productivity
Reference used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 909). McGraw-Hill. Kindle Edition.

NEW QUESTION: 435
When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?
A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
C. They both involve rewriting the media.
D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.
Answer: B (LEAVE A REPLY)
The removal of information from a storage medium is called sanitization.
Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack).
There are three general methods of purging media: overwriting, degaussing, and destruction.
There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There

are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.
Reference(s) use for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 26).
and
A guide to understanding Data Remanence in Automated Information Systems

NEW QUESTION: 436
Which of the following prevents, detects, and corrects errors so that the integrity, availability, and confidentiality of transactions over networks may be maintained?
A. Communications security management and techniques
B. Information security management and techniques
C. Client security management and techniques
D. Server security management and techniques
Answer: A (LEAVE A REPLY)
Communications security and techniques are the best area for addressing this objective.
"Information security management and techniques" is incorrect. While the overall information security program would include this objective, communications security is the more specific and better answer.
"Client security management and techniques" is incorrect. While client security plays a part in this overall objective, communications security is the more specific and better answer.
"Server security management and techniques" is incorrect. While server security plays a part in this overall objective, communications security is the more specific and better answer.
References: CBK, p. 408

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 437
The Secure Hash Algorithm (SHA-1) creates:
A. a fixed length message digest from a fixed length input message

B. a variable length message digest from a variable length input message
C. a fixed length message digest from a variable length input message
D. a variable length message digest from a fixed length input message
Answer: (SHOW ANSWER)
Explanation/Reference:
According to The CISSP Prep Guide, "The Secure Hash Algorithm (SHA-1) computes a fixed length message digest from a variable length input message."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 160.
also see:
http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

NEW QUESTION: 438
Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/software units. Such controls, also known as logical controls, represent which pairing?
A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Technical Pairing
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Preventive/Technical controls are also known as logical controls and can be built into the operating system, be software applications, or can be supplemental hardware/software units.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 439
Why would anomaly detection IDSs often generate a large number of false positives?
A. Because they can only identify correctly attacks they already know about.
B. Because they are application-based are more subject to attacks.
C. Because they can't identify abnormal behavior.
D. Because normal patterns of user and system behavior can vary wildly.
Answer: (SHOW ANSWER)
Section: Analysis and Monitoring
Explanation/Reference:
Unfortunately, anomaly detectors and the Intrusion Detection Systems (IDS) based on them often produce a large number of false alarms, as normal patterns of user and system behavior can vary wildly. Being only able to identify correctly attacks they already know about is a characteristic of misuse detection (signature-based) IDSs. Application-based IDSs are a special subset of host-based IDSs that

analyze the events transpiring within a software application. They are more vulnerable to attacks than host-based IDSs. Not being able to identify abnormal behavior would not cause false positives, since they are not identified.
Source: DUPUIS, Cl?ment, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 92).

NEW QUESTION: 440
Valuable paper insurance coverage does not cover damage to which of the following?
A. Inscribed, printed and Written documents
B. Manuscripts
C. Records
D. Money and Securities
Answer: D (LEAVE A REPLY)
All businesses are driven by records. Even in today's electronic society businesses generate mountains of critical documents everyday. Invoices, client lists, calendars, contracts, files, medical records, and innumerable other records are generated every day.
Stop and ask yourself what happens if your business lost those documents today.
Valuable papers business insurance coverage provides coverage to your business in case of a loss of vital records. Over the years policy language has evolved to include a number of different types of records. Generally, the policy will cover "written, printed, or otherwise inscribed documents and records, including books, maps, films, drawings, abstracts, deeds, mortgages, and manuscripts." But, read the policy coverage carefully. The policy language typically "does not mean "money" or "securities," converted data,programs or instructions used in your data processing operations, including the materials on which the data is recorded."
The coverage is often included as a part of property insurance or as part of a small business owner policy. For example, a small business owner policy includes in many cases valuable papers coverage up to $25,000.
It is important to realize what the coverage actually entails and, even more critical, to analyze your business to determine what it would cost to replace records.
The coverage pays for the loss of vital papers and the cost to replace the records up to the limit of the insurance and after application of any deductible. For example, the insurer will pay to have waterlogged papers dried and reproduced (remember, fires are put out by water and the fire department does not stop to remove your book keeping records). The insurer may cover temporary storage or the cost of moving records to avoid a loss.
For some businesses, losing customer lists, some business records, and contracts, can mean the expense and trouble of having to recreate those documents, but is relatively easy and a low level risk and loss. Larger businesses and especially professionals (lawyers, accountants, doctors) are in an entirely separate category and the cost of replacement of documents is much higher. Consider, in analyzing your business and potential risk, what it would actually cost to reproduce your critical business records. Would you need to hire temporary personnel? How many hours of productivity would go into replacing the

records? Would you need to obtain originals? Would original work need to be recreated (for example, home inspectors, surveyors, cartographers)?
Often when a business owner considers the actual cost related to the reproduction of records, the owner quickly realizes that their business insurance policy limits for valuable papers coverage is woefully inadequate. Insurers (and your insurance professional)will often suggest higher coverages for valuable papers. The extra premium is often worth the cost and should be considered.
Finally, most policies will require records to be protected. You need to review your declarations pages and speak with your insurer to determine what is required. Some insurers may offer discounted coverage if there is a document retention and back up plan in place and followed. There are professional organizations that can assist your business in designing a records management policy to lower the risk (and your premiums). For example, ARMA International has been around since 1955 and its members consist of some of the top document retention and storage companies.
Reference(s) used for this question: http://businessinsure.about.com/od/propertyinsurance/f/vpcov.htm

NEW QUESTION: 441
Which of the following best describes remote journaling?
A. Send hourly tapes containing transactions off-site.
B. Send daily tapes containing transactions off-site.
C. Real-time capture of transactions to multiple storage devices.
D. Real time transmission of copies of the entries in the journal of transactions to an alternate site.
Answer: (SHOW ANSWER)
Explanation/Reference:
Remote Journaling is a technology to facilitate sending copies of the journal of transaction entries from a production system to a secondary system in realtime. The remote nature of such a connection is predicated upon having local journaling already established. Local journaling on the production side allows each change that ensues for a journal-eligible object e.g., database physical file, SQL table, data area, data queue, byte stream file residing within the IFS) to be recorded and logged. It's these local images that flow to the remote system. Once there, the journal entries serve a variety of purposes, from feeding a high availability software replay program or data warehouse to offering an offline, realtime vault of the most recent database changes.
Reference(s) used for this question:
The Essential Guide to Remote Journaling by IBM
and
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 286).

NEW QUESTION: 442

In addition to the Legal Department, with what company function must the collection of physical evidence be coordinated if an employee is suspected?

A. Human Resources

B. Industrial Security

C. Public Relations

D. External Audit Group

Answer: (SHOW ANSWER)

Section: Risk, Response and Recovery

Explanation/Reference:

If an employee is suspected of causing an incident, the human resources department may be involved-for example, in assisting with disciplinary proceedings.

Legal Department. The legal experts should review incident response plans, policies, and procedures to ensure their compliance with law and Federal guidance, including the right to privacy. In addition, the guidance of the general counsel or legal department should be sought if there is reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit, or if there may be a need for a memorandum of understanding (MOU) or other binding agreements involving liability limitations for information sharing.

Public Affairs, Public Relations, and Media Relations. Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public.

The Incident response team members could include:

Management

Information Security

Legal / Human Resources

Public Relations

Communications

Physical Security

Network Security

Network and System Administrators

Network and System Security Administrators

Internal Audit

Events versus Incidents

An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security- related, not those caused by natural disasters, power failures, etc.

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Examples of incidents are:

An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
A user provides or exposes sensitive information to others through peer-to-peer file sharing services.
The following answers are incorrect:
Industrial Security. Is incorrect because it is not the best answer, the human resource department must be involved with the collection of physical evidence if an employee is suspected.
public relations. Is incorrect because it is not the best answer. It would be an important element to minimize public image damage but not the best choice for this question.
External Audit Group. Is incorrect because it is not the best answer, the human resource department must be involved with the collection of physical evidence if an employee is suspected.
Reference(s) used for this question:
NIST Special Publication 800-61

NEW QUESTION: 443
Which of the following embodies all the detailed actions that personnel are required to follow?
A. Standards
B. Guidelines
C. Procedures
D. Baselines
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Procedures are step-by-step instructions in support of of the policies, standards, guidelines and baselines. The procedure indicates how the policy will be implemented and who does what to accomplish the tasks." Standards is incorrect. Standards are a "Mandatory statement of minimum requirements that support some part of a policy, the standards in this case is your own company standards and not standards such as the ISO standards" Guidelines is incorrect. "Guidelines are discretionary or optional controls used to enable individuals to make judgments with respect to security actions." Baselines is incorrect. Baselines "are a minimum acceptable level of security. This minimum is implemented using specific rules necessary to implement the security controls in support of the policy and standards." For example, requiring a password of at leat 8 character would be an example. Requiring all users to have a minimun of an antivirus, a personal firewall, and an anti spyware tool could be another example.
References:
CBK, pp. 12 - 16. Note especially the discussion of the "hammer policy" on pp. 16-17 for the differences between policy, standard, guideline and procedure.
AIO3, pp. 88-93.

NEW QUESTION: 444
Which of the following was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support?
A. SESAME
B. RADIUS
C. KryptoKnight
D. TACACS+
Answer: A (LEAVE A REPLY)
Secure European System for Applications in a Multi-vendor Environment (SESAME) was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support.
Reference:
TIPTON, Harold, Official (ISC)2 Guide to the CISSP CBK (2007), page 184.
ISC OIG Second Edition, Access Controls, Page 111

NEW QUESTION: 445
The following actions have been noted as providing motivation to virus writers? (Choose all that apply)
A. Stupidity
B. Fortune
C. Fame
D. Boredom
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 446
When you update records in multiple locations or you make a copy of the whole database at a remote location as a way to achieve the proper level of fault-tolerance and redundancy, it is knows as?
A. Shadowing
B. Data mirroring
C. Backup
D. Archiving
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Updating records in multiple locations or copying an entire database to a remote location as a means to ensure the appropriate levels of fault-tolerance and redundancy is known as Database shadowing. Shadowing is the technique in which updates are shadowed in multiple locations. It is like copying the entire database on to a remote location.
Shadow files are an exact live copy of the original active database, allowing you to maintain live duplicates of your production database, which can be brought into production in the event of a hardware failure. They are used for security reasons: should the original database be damaged or incapacitated by hardware problems, the shadow can immediately take over as the primary database. It is therefore

important that shadow files do not run on the same server or at least on the same drive as the primary database files.
The following are incorrect answers:
Data mirroring In data storage, disk mirroring is the replication of logical disk volumes onto separate physical hard disks in real time to ensure continuous availability. It is most commonly used in RAID 1. A mirrored volume is a complete logical representation of separate volume copies.
Backups In computing the phrase backup means to copy files to a second medium (a disk or tape) as a precaution in case the first medium fails. One of the cardinal rules in using computers is back up your files regularly. Backups are useful in recovering information or a system in the event of a disaster, else you may be very sorry :-(Archiving is the storage of data that is not in continual use for historical purposes. It is the process of copying files to a long-term storage medium for backup.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 27614-27626). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Disk_mirroring
http://www.webopedia.com/TERM/A/archive.html
http://ibexpert.net/ibe/index.php?n=Doc.DatabaseShadow

NEW QUESTION: 447
Layer 4 in the DoD model overlaps with which layer(s) of the OSI model?
A. Layer 3 - Network Layer
B. Layers 2, 3, & 4 - Data Link, Network, and Transport Layers
C. Layer 7 - Application Layer
D. Layers 5, 6, & 7 - Session, Presentation, and Application Layers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 448
Secure Shell (SSH-2) provides all the following services except:
A. secure remote login
B. command execution
C. port forwarding
D. user authentication
Answer: (SHOW ANSWER)
Explanation/Reference:
This is one of the tricky negative question. You have to pay close attention to the word EXCEPT within the question.
The SSH transport layer is a secure, low level transport protocol. It provides strong encryption, cryptographic host authentication, and integrity protection.
Authentication in this protocol level is host-based; this protocol does not perform user authentication. A higher level protocol for user authentication can be designed on top of this protocol.

The protocol has been designed to be simple and flexible to allow parameter negotiation, and to minimize the number of round-trips. The key exchange method, public key algorithm, symmetric encryption algorithm, message authentication algorithm, and hash algorithm are all negotiated. It is expected that in most environments, only 2 round-trips will be needed for full key exchange, server authentication, service request, and acceptance notification of service request. The worst case is 3 round- trips.
The following are incorrect answers:
"Remote log-on" is incorrect. SSH does provide remote log-on.
"Command execution" is incorrect. SSH does provide command execution.
"Port forwarding" is incorrect. SSH does provide port forwarding. SSH also has a wonderful feature called SSH Port Forwarding, sometimes called SSH Tunneling, which allows you to establish a secure SSH session and then tunnel arbitrary TCP connections through it. Tunnels can be created at any time, with almost no effort and no programming, which makes them very appealing. See the article below in the reference to take a look at SSH Port Forwarding in detail, as it is a very useful but often misunderstood technology. SSH Port Forwarding can be used for secure communications in a myriad of different ways.
You can see a nice tutorial on the PUTTY web site on how to use PUTTY to do port forwarding at:
http://www.cs.uu.nl/technical/services/ssh/putty/puttyfw.html
Reference(s) used for this question:
RFC 4253 at https://www.ietf.org/rfc/rfc4253.txt
and
SSH Port Forwarding by Symantec

NEW QUESTION: 449
What works as an E-mail message transfer agent?
A. SMTP
B. SNMP
C. S-RPC
D. S/MIME
Answer: A (LEAVE A REPLY)
SMTP (Simple Mail Transfer Protocol) works as a message transfer agent. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 821.

NEW QUESTION: 450
Which type of attack would a competitive intelligence attack best classify as?
A. Business attack
B. Intelligence attack
C. Financial attack
D. Grudge attack
Answer: (SHOW ANSWER)
Explanation/Reference:
Business attacks concern information loss through competitive intelligence gathering and computer-related attacks. These attacks can be very costly due the loss of trade secrets and reputation.

Intelligence attacks are aimed at sensitive military and law enforcement files containing military data and investigation reports.
Financial attacks are concerned with frauds to banks and large corporations.
Grudge attacks are targeted at individuals and companies who have done something that the attacker doesn't like.
The CISSP for Dummies book has nice coverage of the different types of attacks, here is an extract:
Terrorism Attacks
Terrorism exists at many levels on the Internet. In April 2001, during a period of tense relations between China and the U.S. (resulting from the crash landing of a U.S. Navy reconnaissance plane on Hainan Island), Chinese hackers (cyberterrorists) launched a major effort to disrupt critical U.S. infrastructure, which included U.S. government and military systems.
Following the terrorist attacks against the U.S. on September 11, 2001, the general public became painfully aware of the extent of terrorism on the Internet. Terrorist organizations and cells are using online capabilities to coordinate attacks, transfer funds, harm international commerce, disrupt critical systems, disseminate propaganda, and gain useful information about developing techniques and instruments of terror, including nuclear , biological, and chemical weapons.
Military and intelligence attacks
Military and intelligence attacks are perpetrated by criminals, traitors, or foreign intelligence agents seeking classified law enforcement or military information. Such attacks may also be carried out by governments during times of war and conflict.
Financial attacks
Banks, large corporations, and e-commerce sites are the targets of financial attacks, all of which are motivated by greed. Financial attacks may seek to steal or embezzle funds, gain access to online financial information, extort individuals or businesses, or obtain the personal credit card numbers of customers.
Business attacks
Businesses are becoming the targets of more and more computer and Internet attacks. These attacks include competitive intelligence gathering, denial of service, and other computer- related attacks.
Businesses are often targeted for several reasons including
Lack of expertise: Despite heightened security awareness, a shortage of qualified security professionals still exists, particularly in private enterprise.
Lack of resources: Businesses often lack the resources to prevent, or even detect, attacks against their systems.
Lack of reporting or prosecution : Because of public relations concerns and the inability to prosecute computer criminals due to either a lack of evidence or a lack of properly handled evidence, the majority of business attacks still go unreported.
The cost to businesses can be significant, including loss of trade secrets or proprietary information, loss of revenue, and loss of reputation.
Grudge attacks

Grudge attacks are targeted at individuals or businesses and are motivated by a desire to take revenge against a person or organization. A disgruntled employee, for example, may steal trade secrets, delete valuable data, or plant a logic bomb in a critical system or application.
Fortunately, these attacks (at least in the case of a disgruntled employee) can be easier to prevent or prosecute than many other types of attacks because:
The attacker is often known to the victim.
The attack has a visible impact that produces a viable evidence trail.
Most businesses (already sensitive to the possibility of wrongful termination suits) have well-established termination procedures
"Fun" attacks
"Fun" attacks are perpetrated by thrill seekers and script kiddies who are motivated by curiosity or excitement. Although these attackers may not intend to do any harm or use any of the information that they access, they're still dangerous and their activities are still illegal.
These attacks can also be relatively easy to detect and prosecute. Because the perpetrators are often script kiddies or otherwise inexperienced hackers, they may not know how to cover their tracks effectively.
Also, because no real harm is normally done nor intended against the system, it may be tempting (although ill advised) for a business to prosecute the individual and put a positive public relations spin on the incident. You've seen the film at 11: "We quickly detected the attack, prevented any harm to our network, and prosecuted the responsible individual; our security is unbreakable !" Such action, however, will likely motivate others to launch a more serious and concerted grudge attack against the business.
Many computer criminals in this category only seek notoriety. Although it's one thing to brag to a small circle of friends about defacing a public Web site, the wily hacker who appears on CNN reaches the next level of hacker celebrity-dom. These twisted individuals want to be caught to revel in their 15 minutes of fame.
References:
ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 10: Law, Investigation, and Ethics (page 187)
and
CISSP Professional Study Guide by James Michael Stewart, Ed Tittel, Mike Chapple, page 607-609 and CISSP for Dummies, Miller L. H. and Gregory P. H. ISBN: 0470537914, page 309-311

NEW QUESTION: 451
Which one of the following statements about the advantages and disadvantages of network-based Intrusion detection systems is true
A. Network-based IDSs are not vulnerable to attacks.
B. Network-based IDSs are well suited for modern switch-based networks.
C. Most network-based IDSs can automatically indicate whether or not an attack was successful.
D. The deployment of network-based IDSs has little impact upon an existing network.
Answer: D (LEAVE A REPLY)
Explanation/Reference:

Network-based IDSs are usually passive devices that listen on a network wire without interfering with the normal operation of a network. Thus, it is usually easy to retrofit a network to include network-based IDSs with minimal effort.
Network-based IDSs are not vulnerable to attacks is not true, even thou network-based IDSs can be made very secure against attack and even made invisible to many attackers they still have to read the packets and sometimes a well crafted packet might exploit or kill your capture engine.
Network-based IDSs are well suited for modern switch-based networks is not true as most switches do not provide universal monitoring ports and this limits the monitoring range of a network-based IDS sensor to a single host. Even when switches provide such monitoring ports, often the single port cannot mirror all traffic traversing the switch.
Most network-based IDSs can automatically indicate whether or not an attack was successful is not true as most network-based IDSs cannot tell whether or not an attack was successful; they can only discern that an attack was initiated. This means that after a network-based IDS detects an attack, administrators must manually investigate each attacked host to determine whether it was indeed penetrated.
Reference:
NIST special publication 800-31 Intrusion Detection System pages 15-16
Official guide to the CISSP CBK. Pages 196 to 197

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 452
The controls that usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists are associated with:
A. Preventive/physical
B. Detective/technical
C. Detective/physical
D. Detective/administrative
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Detective/physical controls usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION: 453
Because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to:
A. neither physical attacks nor attacks from malicious code.
B. physical attacks only
C. both physical attacks and attacks from malicious code.
D. physical attacks but not attacks from malicious code.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Since all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to both physical attacks and attacks from malicious code.
Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

NEW QUESTION: 454
Which of the following services is NOT provided by the digital signature standard (DSS)?
A. Encryption
B. Integrity
C. Digital signature
D. Authentication
Answer: (SHOW ANSWER)
Explanation/Reference:
DSS provides Integrity, digital signature and Authentication, but does not provide Encryption.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 160).

NEW QUESTION: 455
What is the main issue with media reuse?
A. Degaussing
B. Data remanence
C. Media destruction
D. Purging
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:

The main issue with media reuse is data remanence, where residual information still resides on a media that has been erased. Degaussing, purging and destruction are ways to handle media that contains data that is no longer needed or used.
Source: WALLHOFF, John, CBK#10 Physical Security (CISSP Study Guide), April 2002 (page 5).

NEW QUESTION: 456
How often should a Business Continuity Plan be reviewed?
A. At least once a month
B. At least every six months
C. At least once a year
D. At least Quarterly
Answer: (SHOW ANSWER)
Explanation/Reference:
As stated in SP 800-34 Rev. 1:
To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies.
As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency (at least once a year for the purpose of the exam) or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews.
Remember, there could be two good answers as specified above. Either once a year or whenever significant changes occur to the plan. You will of course get only one of the two presented within you exam.
Reference(s) used for this question:
NIST SP 800-34 Revision 1

NEW QUESTION: 457
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system. Acceptable throughput rates are in the range of:
A. 100 subjects per minute.
B. 25 subjects per minute.
C. 10 subjects per minute.
D. 50 subjects per minute.
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system.
Acceptable throughput rates are in the range of 10 subjects per minute.
Things that may impact the throughput rate for some types of biometric systems may include:

A concern with retina scanning systems may be the exchange of body fluids on the eyepiece.
Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 38.

NEW QUESTION: 458
Which of the following is the FIRST step in protecting data's confidentiality?
A. Install a firewall
B. Implement encryption
C. Identify which information is sensitive
D. Review all user access rights
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
In order to protect the confidentiality of the data.
The following answers are incorrect because :
Install a firewall is incorrect as this would come after the information has been identified for sensitivity levels.
Implement encryption is also incorrect as this is one of the mechanisms to protect the data once it has been identified.
Review all user access rights is also incorrect as this is also a protection mechanism for the identified information.
Reference : Shon Harris AIO v3 , Chapter-4 : Access Control , Page : 126

NEW QUESTION: 459
During which phase of an IT system life cycle are security requirements developed?
A. Operation
B. Initiation
C. Functional design analysis and Planning
D. Implementation
Answer: C (LEAVE A REPLY)
The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems.
The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:
This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:
Conduct the risk assessment and use the results to supplement the baseline security controls;
Analyze security requirements;
Perform functional and security testing;

Prepare initial documents for system certification and accreditation; and
Design security architecture.
Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.
Shon Harris' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:
Project initiation Functional design analysis and planning System design specifications Software development Installation Maintenance support Revision and replacement
According to the author (Shon Harris), security requirements should be developed during the functional design analysis and planning phase.
SDLC POSITIONING FROM NIST 800-64
SDLC Positioning in the enterprise Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes to establish insight into the agency's vital business operations, their supporting assets, and existing interdependencies and relationships.
With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program's cost-effective performance as well as articulate its business impact and value to the agency.
SDLC OVERVIEW FROM NIST 800-64 SDLC Overview from NIST 800-64 Revision 2
NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of the phases of the SDLC. You will find a copy at:
http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
DISCUSSION:
Different sources present slightly different info as far as the phases names are concerned. People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development Life Cycle has slightly different names, the activities mostly remains the same.
NIST clearly specifies that Security requirements would be considered throughout ALL of

the phases. The keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the correct choice.
Within the NIST standard they use different phase, howeverr under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it become easier to come out with the answer to this question. Here is what is stated:
The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.
At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage.
By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.
NIST says: NIST`s Information Technology Laboratory recently issued Special Publication (SP) 80064, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.
I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.
References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956 and NIST S-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64Revision2.pdf and http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlcsystem-development

NEW QUESTION: 460
Related to information security, the prevention of the intentional or unintentional unauthorized disclosure of contents is which of the following?
A. Confidentiality
B. Integrity
C. Availability
D. capability
Answer: A (LEAVE A REPLY)
Confidentiality is the prevention of the intentional or unintentional unauthorized disclosure of contents.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 60.

NEW QUESTION: 461

The SubSeven Trojan has been known to exploit which service ports?
A. 6711, 6712, 6776, 27374
B. 137, 139
C. 65000, 65001, 65002
D. 31337, 31338
Answer: A (LEAVE A REPLY)

NEW QUESTION: 462
Who is responsible for initiating corrective measures and capabilities used when there are security violations?
A. Information systems auditor
B. Security administrator
C. Management
D. Data owners
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Management is responsible for protecting all assets that are directly or indirectly under their control. They must ensure that employees understand their obligations to protect the company's assets, and implement security in accordance with the company policy. Finally, management is responsible for initiating corrective actions when there are security violations.
Source: HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

NEW QUESTION: 463
Once evidence is seized, a law enforcement officer should emphasize which of the following?
A. Chain of command
B. Chain of custody
C. Chain of control
D. Chain of communications
Answer: (SHOW ANSWER)
All people that handle the evidence from the time the crime was committed through the final disposition must be identified. This is to ensure that the evidence can be used and has not been tampered with.
The following answers are incorrect:
chain of command. Is incorrect because chain of command is the order of authority and
does not apply to evidence.
chain of control. Is incorrect because it is a distractor.
chain of communications. Is incorrect because it is a distractor.

NEW QUESTION: 464
Which of the following is a token-passing scheme like token ring that also has a second ring that remains dormant until an error condition is detected on the primary ring?
A. Fiber Distributed Data Interface (FDDI).

B. Ethernet
C. Fast Ethernet
D. Broadband
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
FDDI is a token-passing ring scheme like a token ring, yet it also has a second ring that remains dormant until an error condition is detected on the primary ring.
Fiber Distributed Data Interface (FDDI) provides a 100 Mbit/s optical standard for data transmission in a local area network that can extend in range up to 200 kilometers (124 miles). Although FDDI logical topology is a ring-based token network, it does not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol is derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium it uses optical fiber, although it can use copper cable, in which case it may be refer to as CDDI (Copper Distributed Data Interface). FDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology.
Ethernet is a family of frame-based computer networking technologies for local area networks (LANs). The name came from the physical concept of the ether. It defines a number of wiring and signaling standards for the Physical Layer of the OSI networking model as well as a common addressing format and Media Access Control at the Data Link Layer.
In computer networking, Fast Ethernet is a collective term for a number of Ethernet standards that carry traffic at the nominal rate of 100 Mbit/s, against the original Ethernet speed of 10 Mbit/s. Of the fast Ethernet standards 100BASE-TX is by far the most common and is supported by the vast majority of Ethernet hardware currently produced. Fast Ethernet was introduced in 1995 and remained the fastest version of Ethernet for three years before being superseded by gigabit Ethernet.
Broadband in data can refer to broadband networks or broadband Internet and may have the same meaning as above, so that data transmission over a fiber optic cable would be referred to as broadband as compared to a telephone modem operating at 56,000 bits per second. However, a worldwide standard for what level of bandwidth and network speeds actually constitute Broadband have not been determined. [1] Broadband in data communications is frequently used in a more technical sense to refer to data transmission where multiple pieces of data are sent simultaneously to increase the effective rate of transmission, regardless of data signaling rate. In network engineering this term is used for methods where two or more signals share a medium.[Broadband Internet access, often shortened to just broadband, is a high data rate Internet access- typically contrasted with dial-up access using a 56k modem.
Dial-up modems are limited to a bitrate of less than 56 kbit/s (kilobits per second) and require the full use of a telephone line-whereas broadband technologies supply more than double this rate and generally without disrupting telephone use.
Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.

also see:
http://en.wikipedia.org/

NEW QUESTION: 465
Prior to a live disaster test also called a Full Interruption test, which of the following is most important?
A. Restore all files in preparation for the test.
B. Document expected findings.
C. Arrange physical security for the test site.
D. Conduct of a successful Parallel Test
Answer: D (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
A live disaster test or Full interruption test is an actual simulation of the Disaster Recovery Plan. All operations are shut down and brought back online at the alternate site. This test poses the biggest threat to an organization and should not be performed until a successful Parallell Test has been conducted.
1. A Checklist test would be conducted where each of the key players will get a copy of the plan and they read it to make sure it has been properly developed for the specific needs of their departments.
2. A Structure Walk Through would be conducted next. This is when all key players meet together in a room and they walk through the test together to identify shortcoming and dependencies between department.
3. A simulation test would be next. In this case you go through a disaster scenario up to the point where you would move to the alternate site. You do not move to the alternate site and you learn from your mistakes and you improve the plan. It is the right time to find shortcomings.
4. A Parallell Test would be done. You go through a disaster scenario. You move to the alternate site and you process from both sites simultaneously.
5. A full interruption test would be conducted. You move to the alternate site and you resume processing at the alternate site.
The following answers are incorrect:
Restore all files in preparation for the test. Is incorrect because you would restore the files at the alternate site as part of the test not in preparation for the test.
Document expected findings. Is incorrect because it is not the best answer. Documenting the expected findings won't help if you have not performed tests prior to a Full interruption test or live disaster test.
Arrange physical security for the test site. Is incorrect because it is not the best answer. why physical security for the test site is important if you have not performed a successful structured walk-through prior to performing a Full interruption test or live disaster test you might have some unexpected and disasterous results.

NEW QUESTION: 466
Which of the following transmission media would NOT be affected by cross talk or interference?
A. Copper cable
B. Radio System

C. Satellite radiolink
D. Fiber optic cables
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Only fiber optic cables are not affected by crosstalk or interference.
For your exam you should know the information about transmission media:
Copper Cable
Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.
Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.
Copper Cable
Image Source - http://i00.i.aliimg.com/photo/v0/570456138/FRLS_HR_PVC_Copper_Cable.jpg Coaxial cable Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.
Coaxial cable are expensive and does not support many LAN's. It supports data and video Coaxial Cable
Image Source - http://www.tlc-direct.co.uk/Images/Products/size_3/CARG59.JPG Fiber optics An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.
Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.
Radio System
Radio systems are used for short distance,cheap and easy to tap.
Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Fiber Optics

Image Source - http://aboveinfranet.com/wp-content/uploads/2014/04/fiber-optic-cables-above-infranet-solutions.jpg Microwave radio system Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimetre; these are called microwaves.

Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System

Image Source - http://www.valiantcom.com/images/applications/e1_digital_microwave_radio.gif Satellite Radio Link Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to tap.

The following answers are incorrect:

Copper Cable - Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Radio System - Radio systems are used for short distance,cheap and easy to tap.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 265 &

Official ISC2 guide to CISSP CBK 3rd Edition Page number 233

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 467

In which of the following model are Subjects and Objects identified and the permissions applied to each subject/object combination are specified. Such a model can be used to quickly summarize what permissions a subject has for various system objects.

A. Access Control Matrix model

B. Take-Grant model

C. Bell-LaPadula model

D. Biba model

Answer: (SHOW ANSWER)

Explanation/Reference:

An access control matrix is a table of subjects and objects indicating what actions individual subjects can take upon individual objects. Matrices are data structures that programmers implement as table lookups that will be used and enforced by the operating system.

This type of access control is usually an attribute of DAC models. The access rights can be assigned directly to the subjects (capabilities) or to the objects (ACLs).

Capability Table

A capability table specifies the access rights a certain subject possesses pertaining to specific objects. A capability table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.

Access control lists (ACLs)

ACLs are used in several operating systems, applications, and router configurations. They are lists of subjects that are authorized to access a specific object, and they define what level of authorization is granted. Authorization can be specific to an individual, group, or role. ACLs map values from the access control matrix to the object.

Whereas a capability corresponds to a row in the access control matrix, the ACL corresponds to a column of the matrix.

NOTE: Ensure you are familiar with the terms Capability and ACLs for the purpose of the exam.

Resource(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5264-5267). McGraw-Hill. Kindle Edition.

or

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Page 229 and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1923-1925). Auerbach Publications. Kindle Edition.

NEW QUESTION: 468
Which of the following is less likely to be used today in creating a Virtual Private Network?
A. L2TP
B. PPTP
C. IPSec
D. L2F
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
L2F (Layer 2 Forwarding) provides no authentication or encryption. It is a Protocol that supports the creation of secure virtual private dial-up networks over the Internet.
At one point L2F was merged with PPTP to produce L2TP to be used on networks and not only on dial up links.
IPSec is now considered the best VPN solution for IP environments.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 8:
Cryptography (page 507).

NEW QUESTION: 469
What algorithm has been selected as the AES algorithm, replacing the DES algorithm?
A. RC6
B. Twofish
C. Rijndael
D. Blowfish
Answer: C (LEAVE A REPLY)
Explanation/Reference:
On October 2, 2000, NIST announced the selection of the Rijndael Block Cipher, developed by the Belgian cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen, as the proposed AES algorithm. Twofish and RC6 were also candidates. Blowfish is also a symmetric algorithm but wasn't a finalist for a replacement for DES.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 152).

NEW QUESTION: 470
A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed:
A. at one end of the connection.
B. at both ends of the connection.

C. somewhere between both end points.
D. in the middle of the connection.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
A common way to create fault tolerance with leased lines is to group several T1s together with an inverse multiplexer placed at both ends of the connection.
In fact it would be a Multiplexer at one end and DeMultiplexer at other end or vice versa. Inverse Multiplexer at both end.
In electronics, a multiplexer (or mux) is a device that selects one of several analog or digital input signals and forwards the selected input into a single line. A multiplexer of 2n inputs has n select lines, which are used to select which input line to send to the output. Multiplexers are mainly used to increase the amount of data that can be sent over the network within a certain amount of time and bandwidth. A multiplexer is also called a data selector.
An electronic multiplexer makes it possible for several signals to share one device or resource, for example one A/D converter or one communication line, instead of having one device per input signal.
On the other hand, a demultiplexer (or demux) is a device taking a single input signal and selecting one of many data-output-lines, which is connected to the single input. A multiplexer is often used with a complementary demultiplexer on the receiving end.
An electronic multiplexer can be considered as a multiple-input, single-output switch, and a demultiplexer as a single-input, multiple-output switch
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.
and
https://secure.wikimedia.org/wikipedia/en/wiki/Multiplexer

NEW QUESTION: 471
A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:
A. concern that the laser beam may cause eye damage
B. the iris pattern changes as a person grows older.
C. there is a relatively high rate of false accepts.
D. the optical unit must be positioned so that the sun does not shine into the aperture.
Answer: D (LEAVE A REPLY)
Because the optical unit utilizes a camera and infrared light to create the
images, sun light can impact the aperture so it must not be positioned in direct light of any
type. Because the subject does not need to have direct contact with the optical reader,
direct light can impact the reader.
An Iris recognition is a form of biometrics that is based on the uniqueness of a subject's iris.
A camera like device records the patterns of the iris creating what is known as Iriscode.
It is the unique patterns of the iris that allow it to be one of the most accurate forms of

biometric identification of an individual. Unlike other types of biometics, the iris rarely changes over time. Fingerprints can change over time due to scaring and manual labor, voice patterns can change due to a variety of causes, hand geometry can also change as well. But barring surgery or an accident it is not usual for an iris to change. The subject has a high-resoulution image taken of their iris and this is then converted to Iriscode. The current standard for the Iriscode was developed by John Daugman. When the subject attempts to be authenticated an infrared light is used to capture the iris image and this image is then compared to the Iriscode. If there is a match the subject's identity is confirmed. The subject does not need to have direct contact with the optical reader so it is a less invasive means of authentication then retinal scanning would be.
Reference(s) used for this question:
AIO, 3rd edition, Access Control, p 134.
AIO, 4th edition, Access Control, p 182.
Wikipedia - http://en.wikipedia.org/wiki/Iris_recognition
The following answers are incorrect:
concern that the laser beam may cause eye damage. The optical readers do not use laser so, concern that the laser beam may cause eye damage is not an issue.
the iris pattern changes as a person grows older. The question asked about the physical installation of the scanner, so this was not the best answer. If the question would have been about long term problems then it could have been the best choice. Recent research has shown that Irises actually do change over time: http://www.nature.com/news/ageingeyes-hinder-biometric-scans-1.10722
there is a relatively high rate of false accepts. Since the advent of the Iriscode there is a very low rate of false accepts, in fact the algorithm used has never had a false match. This all depends on the quality of the equipment used but because of the uniqueness of the iris even when comparing identical twins, iris patterns are unique.

NEW QUESTION: 472
What is called a password that is the same for each log-on session?
A. "one-time password"
B. "two-time password"
C. static password
D. dynamic password
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION: 473
Which of the following statements pertaining to key management is incorrect?
A. The more a key is used, the shorter its lifetime should be.

B. When not using the full keyspace, the key should be extremely random.
C. Keys should be backed up or escrowed in case of emergencies.
D. A key's lifetime should correspond with the sensitivity of the data it is protecting.
Answer: B (LEAVE A REPLY)
Section: Cryptography
Explanation
Explanation/Reference:
A key should always be using the full spectrum of the keyspace and be extremely random. Other statements are correct.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

NEW QUESTION: 474
Select the major difference(s) between block and stream ciphers. (Choose all that apply)
A. Block = hardware driven; stream = software driven
B. Block = slower encryption; stream = fast encryption
C. Stream = hardware driven; block = software driven
D. Block = bit by bit = encrypted in equal sections
E. Streams = bit by bit; block = encrypted in equal sections
Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 475
A Business Continuity Plan should be tested:
A. Once a month.
B. At least twice a year.
C. At least once a year.
D. At least once every two years.
Answer: C (LEAVE A REPLY)
It is recommended that testing does not exceed established frequency limits. For a plan to be effective, all components of the BCP should be tested at least once a year. Also, if there is a major change in the operations of the organization, the plan should be revised and tested not more than three months after the change becomes operational.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 165).

NEW QUESTION: 476
In a hierarchical PKI the highest CA is regularly called Root CA, it is also referred to by which one of the following term?
A. Subordinate CA
B. Top Level CA
C. Big CA
D. Master CA

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Reference: Arsenault, Turner, Internet X.509 Public Key Infrastructure: Roadmap, Chapter "Terminology". Also note that sometimes other terms such as Certification Authority Anchor (CAA) might be used within some government organization, Top level CA is another common term to indicate the top level CA, Top Level Anchor could also be used.

NEW QUESTION: 477

Which of the following would be true about Static password tokens?

A. The owner identity is authenticated by the token

B. The owner will never be authenticated by the token.

C. The owner will authenticate himself to the system.

D. The token does not authenticates the token owner but the system.

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Password Tokens

Tokens are electronic devices or cards that supply a user's password for them. A token system can be used to supply either a static or a dynamic password. There is a big difference between the static and dynamic systems, a static system will normally log a user in but a dynamic system the user will often have to log themselves in.

Static Password Tokens:

The owner identity is authenticated by the token. This is done by the person who issues the token to the owner (normally the employer). The owner of the token is now authenticated by "something you have". The token authenticates the identity of the owner to the information system. An example of this occurring is when an employee swipes his or her smart card over an electronic lock to gain access to a store room.

Synchronous Dynamic Password Tokens:

This system is a lot more complex then the static token password. The synchronous dynamic password tokens generate new passwords at certain time intervals that are synched with the main system. The password is generated on a small device similar to a pager or a calculator that can often be attached to the user's key ring. Each password is only valid for a certain time period, typing in the wrong password in the wrong time period will invalidate the authentication. The time factor can also be the systems downfall. If a clock on the system or the password token device becomes out of synch, a user can have troubles authenticating themselves to the system.

Asynchronous Dynamic Password Tokens:

The clock synching problem is eliminated with asynchronous dynamic password tokens. This system works on the same principal as the synchronous one but it does not have a time frame. A lot of big companies use this system especially for employee's who may work from home on the companies VPN (Virtual private Network).

Challenge Response Tokens:

This is an interesting system. A user will be sent special "challenge" strings at either random or timed intervals. The user inputs this challenge string into their token device and the device will respond by

generating a challenge response. The user then types this response into the system and if it is correct they are authenticated.
Reference(s) used for this question:
http://www.informit.com/guides/content.aspx?g=security&seqNum=146
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION: 478
Which of the following is NOT a characteristic of a host-based intrusion detection system?
A. A HIDS does not consume large amounts of system resources
B. A HIDS can analyse system logs, processes and resources
C. A HIDS looks for unauthorized changes to the system
D. A HIDS can notify system administrators when unusual events are identified
Answer: A (LEAVE A REPLY)
Explanation/Reference:
A HIDS does not consume large amounts of system resources is the correct choice. HIDS can consume inordinate amounts of CPU and system resources in order to function effectively, especially during an event.
All the other answers are characteristics of HIDSes
A HIDS can:
scrutinize event logs, critical system files, and other auditable system resources; look for unauthorized change or suspicious patterns of behavior or activity can send alerts when unusual events are discovered
Reference:
Official guide to the CISSP CBK. Pages 197 to 198.

NEW QUESTION: 479
Which of the following is NOT part of the Kerberos authentication protocol?
A. Symmetric key cryptography
B. Authentication service (AS)
C. Principals
D. Public Key
Answer: D (LEAVE A REPLY)
Explanation/Reference:
There is no such component within kerberos environment. Kerberos uses only symmetric encryption and does not make use of any public key component.
The other answers are incorrect because :
Symmetric key cryptography is a part of Kerberos as the KDC holds all the users' and services' secret keys.

Authentication service (AS) : KDC (Key Distribution Center) provides an authentication service
Principals : Key Distribution Center provides services to principals , which can be users , applications or network services.
References: Shon Harris , AIO v3 , Chapter - 4: Access Control , Pages : 152-155.

NEW QUESTION: 480
CORRECT TEXT
If Big Texastelephone company suddenly started billing you for caller ID and call forwarding without your permission, this practice is referred to as _____.
Answer:

NEW QUESTION: 481
A group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability is:
A. server cluster
B. client cluster
C. guest cluster
D. host cluster
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
A server cluster is a group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 67.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 482
Communications and network security relates to transmission of which of the following?
A. voice
B. voice and multimedia
C. data and multimedia
D. voice, data and multimedia

Answer: B (LEAVE A REPLY)
Explanation/Reference:
From the published (ISC)2 goals for the Certified Information Systems Security Professional candidate: The CISSP candidate should be familiar to communications and network security as it relates to voice, data, multimedia, and facsimile transmissions in terms of local area, wide area, and remote access.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 57.

NEW QUESTION: 483
CORRECT TEXT
_____ is a high speed data routing technology also known as X.25.
Answer:
Switching

NEW QUESTION: 484
An alternative to using passwords for authentication in logical or technical access control is:
A. manage without passwords
B. biometrics
C. not there
D. use of them for physical access control
Answer: B (LEAVE A REPLY)
Explanation/Reference:
An alternative to using passwords for authentication in logical or technical access control is biometrics. Biometrics are based on the Type 3 authentication mechanism-something you are.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION: 485
A trusted system does NOT involve which of the following?
A. Enforcement of a security policy.
B. Sufficiency and effectiveness of mechanisms to be able to enforce a security policy.
C. Assurance that the security policy can be enforced in an efficient and reliable manner.
D. Independently-verifiable evidence that the security policy-enforcing mechanisms are sufficient and effective.
Answer: (SHOW ANSWER)
Explanation/Reference:
A trusted system is one that meets its intended security requirements. It involves sufficiency and effectiveness, not necessarily efficiency, in enforcing a security policy. Put succinctly, trusted systems have (1) policy, (2) mechanism, and (3) assurance.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION: 486
Which of the following is a method of multiplexing data where a communication channel is divided into an arbitrary number of variable bit-rate digital channels or data streams. This method allocates bandwidth dynamically to physical channels having information to transmit?
A. Time-division multiplexing
B. Asynchronous time-division multiplexing
C. Statistical multiplexing
D. Frequency division multiplexing
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Statistical multiplexing is a type of communication link sharing, very similar to dynamic bandwidth allocation (DBA). In statistical multiplexing, a communication channel is divided into an arbitrary number of variable bit- rate digital channels or data streams. The link sharing is adapted to the instantaneous traffic demands of the data streams that are transferred over each channel. This is an alternative to creating a fixed sharing of a link, such as in general time division multiplexing (TDM) and frequency division multiplexing (FDM). When performed correctly, statistical multiplexing can provide a link utilization improvement, called the statistical multiplexing gain.
Generally, the methods for multiplexing data include the following :
Time-division multiplexing (TDM): information from each data channel is allocated bandwidth based on pre- assigned time slots, regardless of whether there is data to transmit. Time-division multiplexing is used primarily for digital signals, but may be applied in analog multiplexing in which two or more signals or bit streams are transferred appearing simultaneously as sub-channels in one communication channel, but are physically taking turns on the channel. The time domain is divided into several recurrent time slots of fixed length, one for each sub-channel. A sample byte or data block of sub-channel 1 is transmitted during time slot
1, sub-channel 2 during time slot 2, etc. One TDM frame consists of one time slot per sub-channel plus a synchronization channel and sometimes error correction channel before the synchronization. After the last sub- channel, error correction, and synchronization, the cycle starts all over again with a new frame, starting with the second sample, byte or data block from sub-channel 1, etc.
Asynchronous time-division multiplexing (ATDM): information from data channels is allocated bandwidth as needed, via dynamically assigned time slots. ATM provides functionality that is similar to both circuit switching and packet switching networks: ATM uses asynchronous time-division multiplexing, and encodes data into small, fixed-sized packets (ISO-OSI frames) called cells. This differs from approaches such as the Internet Protocol or Ethernet that use variable sized packets and frames. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.
These virtual circuits may be "permanent", i.e. dedicated connections that are usually preconfigured by the service provider, or "switched", i.e. set up on a per-call basis using signalling and disconnected when the call is terminated.

Frequency division multiplexing (FDM): information from each data channel is allocated bandwidth based on the signal frequency of the traffic. In telecommunications, frequency-division multiplexing (FDM) is a technique by which the total bandwidth available in a communication medium is divided into a series of non-overlapping frequency sub-bands, each of which is used to carry a separate signal. This allows a single transmission medium such as the radio spectrum, a cable or optical fiber to be shared by many signals.
Reference used for this question:
http://en.wikipedia.org/wiki/Statistical_multiplexing
and
http://en.wikipedia.org/wiki/Frequency_division_multiplexing
and
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 114).

NEW QUESTION: 487
Which layer of the DoD TCP/IP Model ensures error-free delivery and packet sequencing?
A. Internet layer
B. Network access layer
C. Host-to-host
D. Application layer
Answer: (SHOW ANSWER)
Explanation/Reference:
This layer of the DoD Model is also sometimes called Transport in some books but the proper name is Host-to-Host as per the RFC document.
The host-to-host layer provides for reliable end-to-end communications, ensures the data's error-free delivery, handles the data's packet sequencing, and maintains the data's integrity.
It is comparable to the transport layer of the OSI model.
Reference(s) used for this question:
http://en.wikipedia.org/wiki/Internet_protocol_suite
and
http://technet.microsoft.com/en-us/library/cc786900%28v=ws.10%29.aspx
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 85).

NEW QUESTION: 488
Which of the following is NOT a known type of Message Authentication Code (MAC)?
A. Keyed-hash message authentication code (HMAC)
B. DES-CBC
C. Signature-based MAC (SMAC)

D. Universal Hashing Based MAC (UMAC)

Answer: (SHOW ANSWER)

Explanation/Reference:

There is no such thing as a Signature-Based MAC. Being the wrong choice in the list, it is the best answer to this question.

WHAT IS A Message Authentication Code (MAC)?

In Cryptography, a MAC (Message Authentication Code) also known as a cryptographic checksum, is a small block of data that is generated using a secret key and then appended to the message. When the message is received, the recipient can generate their own MAC using the secret key, and thereby know that the message has not changed either accidentally or intentionally in transit. Of course, this assurance is only as strong as the trust that the two parties have that no one else has access to the secret key.

A MAC is a small representation of a message and has the following characteristics:

A MAC is much smaller than the message generating it.

Given a MAC, it is impractical to compute the message that generated it.

Given a MAC and the message that generated it, it is impractical to find another message generating the same MAC.

See the graphic below from Wikipedia showing the creation of a MAC value:

Message Authentication Code MAC HMAC

In the example above, the sender of a message runs it through a MAC algorithm to produce a MAC data tag. The message and the MAC tag are then sent to the receiver. The receiver in turn runs the message portion of the transmission through the same MAC algorithm using the same key, producing a second MAC data tag. The receiver then compares the first MAC tag received in the transmission to the second generated MAC tag. If they are identical, the receiver can safely assume that the integrity of the message was not compromised, and the message was not altered or tampered with during transmission.

However, to allow the receiver to be able to detect replay attacks, the message itself must contain data that assures that this same message can only be sent once (e.g. time stamp, sequence number or use of a one-time MAC). Otherwise an attacker could - without even understanding its content - record this message and play it back at a later time, producing the same result as the original sender.

NOTE: There are many ways of producing a MAC value. Below you have a short list of some implementation.

The following were incorrect answers for this question:

They were all incorrect answers because they are all real type of MAC implementation.

In the case of DES-CBC, a MAC is generated using the DES algorithm in CBC mode, and the secret DES key is shared by the sender and the receiver. The MAC is actually just the last block of ciphertext generated by the algorithm. This block of data (64 bits) is attached to the unencrypted message and transmitted to the far end. All previous blocks of encrypted data are discarded to prevent any attack on the MAC itself. The receiver can just generate his own MAC using the secret DES key he shares to ensure message integrity and authentication. He knows that the message has not changed because the chaining function of CBC would significantly alter the last block of data if any bit had changed anywhere in the message. He knows the source of the message (authentication) because only one other person holds the secret key.

A Keyed-hash message authentication code (HMAC) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as MD5, SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly.
The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key.
A message authentication code based on universal hashing, or UMAC, is a type of message authentication code (MAC) calculated choosing a hash function from a class of hash functions according to some secret (random) process and applying it to the message. The resulting digest or fingerprint is then encrypted to hide the identity of the hash function used. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. UMAC is specified in RFC 4418, it has provable cryptographic strength and is usually a lot less computationally intensive than other MACs.
What is the MicMac (confusion) with MIC and MAC?
The term message integrity code (MIC) is frequently substituted for the term MAC, especially in communications, where the acronym MAC traditionally stands for Media Access Control when referring to Networking. However, some authors use MIC as a distinctly different term from a MAC; in their usage of the term the MIC operation does not use secret keys. This lack of security means that any MIC intended for use gauging message integrity should be encrypted or otherwise be protected against tampering. MIC algorithms are created such that a given message will always produce the same MIC assuming the same algorithm is used to generate both. Conversely, MAC algorithms are designed to produce matching MACs only if the same message, secret key and initialization vector are input to the same algorithm. MICs do not use secret keys and, when taken on their own, are therefore a much less reliable gauge of message integrity than MACs. Because MACs use secret keys, they do not necessarily need to be encrypted to provide the same level of assurance.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 15799-15815). Auerbach Publications. Kindle Edition.
and
http://en.wikipedia.org/wiki/Message_authentication_code
and
http://tools.ietf.org/html/rfc4418

NEW QUESTION: 489
Which of the following is NOT a compensating measure for access violations?
A. Backups
B. Business continuity planning
C. Insurance
D. Security awareness

Answer: D (LEAVE A REPLY)
Security awareness is a preventive measure, not a compensating measure for access violations. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 50).

NEW QUESTION: 490
Which of the following tasks is NOT usually part of a Business Impact Analysis (BIA)?
A. Calculate the risk for each different business function.
B. Identify the company's critical business functions.
C. Calculate how long these functions can survive without these resources.
D. Develop a mission statement.
Answer: D (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The Business Impact Analysis is critical for the development of a business continuity plan (BCP). It identifies risks, critical processes and resources needed in case of recovery and quantifies the impact a disaster will have upon the organization. The development of a mission statement is normally performed before the BIA.
A BIA (business impact analysis) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions ; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level.
BIA Steps
The more detailed and granular steps of a BIA are outlined here:
1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Location 21076). Auerbach Publications. Kindle Edition.
and
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 905-910). McGraw-Hill. Kindle Edition.

NEW QUESTION: 491
Which of the following statements pertaining to disaster recovery planning is incorrect?

A. Every organization must have a disaster recovery plan
B. A disaster recovery plan contains actions to be taken before, during and after a disruptive event.
C. The major goal of disaster recovery planning is to provide an organized way to make decisions if a disruptive event occurs.
D. A disaster recovery plan should cover return from alternate facilities to primary facilities.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
It is possible that an organization may not need a disaster recovery plan. An organization may not have any critical processing areas or system and they would be able to withstand lengthy interruptions.
Remember that DRP is related to systems needed to support your most critical business functions.
The DRP plan covers actions to be taken when a disaster occur but DRP PLANNING which is the keywork in the question would also include steps that happen before you use the plan such as development of the plan, training, drills, logistics, and a lot more.
To be effective, the plan would certainly cover before, during, and after the disaster actions.
It may take you a couple years to develop a plan for a medium size company, there is a lot that has to happen before the plan would be actually used in a real disaster scenario. Plan for the worst and hope for the best.
All other statements are true.
NOTE FROM CLEMENT:
Below is a great article on who legally needs a plan which is very much in line with this question. Does EVERY company needs a plan? The legal answer is NO. Some companies, industries, will be required according to laws or regulations to have a plan. A blank statement saying: All companies MUST have a plan would not be accurate. The article below is specific to the USA but similar laws will exist in many other countries.
Some companies such as utilities, power, etc... might also need plan if they have been defined as Critical Infrastructure by the government. The legal side of IT is always very complex and varies in different countries. Always talk to your lawyer to ensure you follow the law of the land :-) Read the details below:
So Who, Legally, MUST Plan?
With the caveats above, let's cover a few of the common laws where there is a duty to have a disaster recovery plan. I will try to include the basis for that requirement, where there is an implied mandate to do so, and what the difference is between the two
Banks and Financial Institutions MUST Have a Plan
The Federal Financial Institutions Examination Council (Council) was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. In 1989, Title XI of the Financial Institutions Reform, Recovery and Enforcement Act of
1989 (FIRREA) established the Examination Council (the Council).
The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift

Supervision (OTS); and to make recommendations to promote uniformity in the supervision of financial institutions. In other words, every bank, savings and loan, credit union, and other financial institution is governed by the principles adopted by the Council.

In March of 2003, the Council released its Business Continuity Planning handbook designed to provide guidance and examination procedures for examiners in evaluating financial institution and service provider risk-management processes.

Stockbrokers MUST Have a Plan

The National Association of Securities Dealers (NASD) has adopted rules that require all its members to have business continuity plans. The NASD oversees the activities of more than 5,100 brokerage firms, approximately 130,800 branch offices and more than 658,770 registered securities representatives.

As of June 14, 2004, the rules apply to all NASD member firms. The requirements, which are specified in Rule 3510, begin with the following:

3510. Business Continuity Plans. (a) Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member to meet its existing obligations to customers. In addition, such procedures must address the member's existing relationships with other broker-dealers and counter-parties. The business continuity plan must be made available promptly upon request to NASD staff.

NOTE:

The rules apply to every company that deals in securities, such as brokers, dealers, and their representatives, it does NOT apply to the listed companies themselves.

Electric Utilities WILL Need a Plan

The disaster recovery function relating to the electric utility grid is presently undergoing a change. Prior to 2005, the Federal Energy Regulatory Commission (FERC) could only coordinate volunteer efforts between utilities. This has changed with the adoption of Title XII of the Energy Policy Act of 2005 (16 U.S.C. 824o).

That new law authorizes the FERC to create an Electric Reliability Organization (ERO).

The ERO will have the capability to adopt and enforce reliability standards for "all users, owners, and operators of the bulk power system" in the United States. At this time, FERC is in the process of finalizing the rules for the creation of the ERO. Once the ERO is created, it will begin the process of establishing reliability standards.

It is very safe to assume that the ERO will adopt standards for service restoration and disaster recovery, particularly after such widespread disasters as Hurricane Katrina.

Telecommunications Utilities SHOULD Have Plans, but MIGHT NOT

Telecommunications utilities are governed on the federal level by the Federal Communications Commission (FCC) for interstate services and by state Public Utility Commissions (PUCs) for services within the state.

The FCC has created the Network Reliability and Interoperability Council (NRIC). The role of the NRIC is to develop recommendations for the FCC and the telecommunications industry to "insure [sic] optimal reliability, security, interoperability and interconnectivity of, and accessibility to, public communications networks and the internet." The NRIC members are senior representatives of providers and users of

telecommunications services and products, including telecommunications carriers, the satellite, cable television, wireless and computer industries, trade associations, labor and consumer representatives, manufacturers, research organizations, and government-related organizations.

There is no explicit provision that we could find that says telecommunications carriers must have a Disaster Recovery Plan. As I have stated frequently in this series of articles on disaster recovery, however, telecommunications facilities are tempting targets for terrorism. I have not changed my mind in that regard and urge caution.

You might also want to consider what the liability of a telephone company is if it does have a disaster that causes loss to your organization. In three words: It's not much. The following is the statement used in most telephone company tariffs with regard to its liability:

The Telephone Company's liability, if any, for its gross negligence or willful misconduct is not limited by this tariff. With respect to any other claim or suit, by a customer or any others, for damages arising out of mistakes, omissions, interruptions, delays or errors, or defects in transmission occurring in the course of furnishing services hereunder, the Telephone Company's liability, if any, shall not exceed an amount equivalent to the proportionate charge to the customer for the period of service during which such mistake, omission, interruption, delay, error or defect in transmission or service occurs and continues.

(Source, General Exchange Tariff for major carrier)

All Health Care Providers WILL Need a Disaster Recovery Plan

HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, which amended the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act, the Act includes a section, Title II, entitled Administrative Simplification, requiring "Improved efficiency in healthcare delivery by standardizing electronic data interchange, and protection of confidentiality and security of health data through setting and enforcing standards."

The legislation called upon the Department of Health and Human Services (HHS) to publish new rules that will ensure security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present, or future.

The final Security Rule was published by HHS on February 20, 2003 and provides for a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual.

The Security Rule requires covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) that the covered entity creates, receives, maintains, or transmits. It also requires entities to protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule, and ensure compliance by their workforce.

Required safeguards include application of appropriate policies and procedures, safeguarding physical access to ePHI, and ensuring that technical security measures are in place to protect networks, computers and other electronic devices.

Companies with More than 10 Employees

The United States Department of Labor has adopted numerous rules and regulations in regard to workplace safety as part of the Occupational Safety and Health Act. For example, 29 USC 654 specifically requires:
(a) Each employer:
(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;
(2) shall comply with occupational safety and health standards promulgated under this Act.
(b) Each employee shall comply with occupational safety and health standards and all rules, regulations, and orders issued pursuant to this Act which are applicable to his own actions and conduct.
Other Considerations or Expensive Research Qs for Lawyers (Sorry, Eddie!) The Foreign Corrupt Practices Act of 1977
Internal Revenue Service (IRS) Law for Protecting Taxpayer Information
Food and Drug Administration (FDA) Mandated Requirements
Homeland Security and Terrorist Prevention
Pandemic (Bird Flu) Prevention
ISO 9000 Certification
Requirements for Radio and TV Broadcasters
Contract Obligations to Customers
Document Protection and Retention Laws
Personal Identity Theft...and MORE!
Suffice it to say you will need to check with your legal department for specific requirements in your business and industry!
I would like to thank my good friend, Eddie M. Pope, for his insightful contributions to this article, our upcoming book, and my ever-growing pool of lawyer jokes. If you want more information on the legal aspects of recovery planning, Eddie can be contacted at my company or via email at mailto:mempope@tellawcomlabs.com. (Eddie cannot, of course, give you legal advice, but he can point you in the right direction.)
I hope this article helps you better understand the complex realities of the legal reasons why we plan and wish you the best of luck
See original article at: http://www.informit.com/articles/article.aspx?p=777896 See another interesting article on the subject at: http://www.informit.com/articles/article.aspx?p=677910&seqNum=1
References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 281).

NEW QUESTION: 492
Rule-Based Access Control (RuBAC) access is determined by rules. Such rules would fit within what category of access control ?

A. Discretionary Access Control (DAC)
B. Mandatory Access control (MAC)
C. Non-Discretionary Access Control (NDAC)
D. Lattice-based Access control
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Rule-based access control is a type of non-discretionary access control because this access is determined by rules and the subject does not decide what those rules will be, the rules are uniformly applied to ALL of the users or subjects.
In general, all access control policies other than DAC are grouped in the category of non-discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action.
Both Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC) fall within Non Discretionary Access Control (NDAC). If it is not DAC or MAC then it is most likely NDAC.
IT IS NOT ALWAYS BLACK OR WHITE
The different access control models are not totally exclusive of each others. MAC is making use of Rules to be implemented. However with MAC you have requirements above and beyond having simple access rules. The subject would get formal approval from management, the subject must have the proper security clearance, objects must have labels/sensitivity levels attached to them, subjects must have the proper security clearance. If all of this is in place then you have MAC.
BELOW YOU HAVE A DESCRIPTION OF THE DIFFERENT CATEGORIES:
MAC = Mandatory Access Control
Under a mandatory access control environment, the system or security administrator will define what permissions subjects have on objects. The administrator does not dictate user's access but simply configure the proper level of access as dictated by the Data Owner.
The MAC system will look at the Security Clearance of the subject and compare it with the object sensitivity level or classification level. This is what is called the dominance relationship.
The subject must DOMINATE the object sensitivity level. Which means that the subject must have a security clearance equal or higher than the object he is attempting to access.
MAC also introduce the concept of labels. Every objects will have a label attached to them indicating the classification of the object as well as categories that are used to impose the need to know (NTK) principle.
Even thou a user has a security clearance of Secret it does not mean he would be able to access any Secret documents within the system. He would be allowed to access only Secret document for which he has a Need To Know, formal approval, and object where the user belong to one of the categories attached to the object.
If there is no clearance and no labels then IT IS NOT Mandatory Access Control.
Many of the other models can mimic MAC but none of them have labels and a dominance relationship so they are NOT in the MAC category.
NISTR-7316 Says:

Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the "simple security rule," or "no read up." Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the "*-property" (pronounced "star property") or "no write down." The *-property is required to maintain system security in an automated environment. A variation on this rule called the "strict *-property" requires that information can be written at, but not above, the subject's clearance level. Multilevel security models such as the Bell-La Padula Confidentiality and Biba Integrity models are used to formally specify this kind of MAC policy.
DAC = Discretionary Access Control
DAC is also known as: Identity Based access control system.
The owner of an object is define as the person who created the object. As such the owner has the discretion to grant access to other users on the network. Access will be granted based solely on the identity of those users.
Such system is good for low level of security. One of the major problem is the fact that a user who has access to someone's else file can further share the file with other users without the knowledge or permission of the owner of the file. Very quickly this could become the wild wild west as there is no control on the dissimination of the information.
RBAC = Role Based Access Control
RBAC is a form of Non-Discretionary access control.
Role Based access control usually maps directly with the different types of jobs performed by employees within a company.
For example there might be 5 security administrator within your company. Instead of creating each of their profile one by one, you would simply create a role and assign the administrators to the role. Once an administrator has been assigned to a role, he will IMPLICITLY inherit the permissions of that role.
RBAC is great tool for environment where there is a a large rotation of employees on a daily basis such as a very large help desk for example.
RBAC or RuBAC = Rule Based Access Control
RuBAC is a form of Non-Discretionary access control.
A good example of a Rule Based access control device would be a Firewall. A single set of rules is imposed to all users attempting to connect through the firewall.
NOTE FROM CLEMENT:
Lot of people tend to confuse MAC and Rule Based Access Control.
Mandatory Access Control must make use of LABELS. If there is only rules and no label, it cannot be Mandatory Access Control. This is why they call it Non Discretionary Access control (NDAC).
There are even books out there that are WRONG on this subject. Books are sometimes opiniated and not strictly based on facts.
In MAC subjects must have clearance to access sensitive objects. Objects have labels that contain the classification to indicate the sensitivity of the object and the label also has categories to enforce the need to know.

Today the best example of rule based access control would be a firewall. All rules are imposed globally to any user attempting to connect through the device. This is NOT the case with MAC.
I strongly recommend you read carefully the following document:
NISTIR-7316 at http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf It is one of the best Access Control Study document to prepare for the exam. Usually I tell people not to worry about the hundreds of NIST documents and other reference. This document is an exception. Take some time to read it.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.
and
NISTIR-7316 at http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf and
Conrad, Eric; Misenar, Seth; Feldman, Joshua (2012-09-01). CISSP Study Guide (Kindle Locations 651-652). Elsevier Science (reference). Kindle Edition.

NEW QUESTION: 493
Which of the following access control models requires defining classification for objects?
A. Role-based access control
B. Discretionary access control
C. Identity-based access control
D. Mandatory access control
Answer: D (LEAVE A REPLY)
With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and classification of objects.
The Following answers were incorrect:
Identity-based Access Control is a type of Discretionary Access Control (DAC), they are synonymous.
Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC or RBAC) are types of Non Discretionary Access Control (NDAC).
Tip:
When you have two answers that are synonymous they are not the right choice for sure.
There is only one access control model that makes use of Label, Clearances, and Categories, it is Mandatory Access Control, none of the other one makes use of those items.
Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION: 494
Which of the following tasks is NOT usually part of a Business Impact Analysis (BIA)?

A. Calculate the risk for each different business function.
B. Identify the company's critical business functions.
C. Calculate how long these functions can survive without these resources.
D. Develop a mission statement.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
The Business Impact Analysis is critical for the development of a business continuity plan (BCP). It identifies risks, critical processes and resources needed in case of recovery and quantifies the impact a disaster will have upon the organization. The development of a mission statement is normally performed before the BIA.
A BIA (business impact analysis) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions ; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level.
BIA Steps
The more detailed and granular steps of a BIA are outlined here:
1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Location 21076). Auerbach Publications. Kindle Edition.
and
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 905-910). McGraw-Hill. Kindle Edition.

NEW QUESTION: 495
What does "System Integrity" mean?
A. The software of the system has been implemented as designed.
B. Users can't tamper with processes they do not own.
C. Hardware and firmware have undergone periodic testing to verify that they are functioning properly.
D. Design specifications have been verified against the formal top-level specification.
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation
Explanation/Reference:

System Integrity means that all components of the system cannot be tampered with by unauthorized personnel and can be verified that they work properly.
The following answers are incorrect:
The software of the system has been implemented as designed. Is incorrect because this would fall under Trusted system distribution.
Users can't tamper with processes they do not own. Is incorrect because this would fall under Configuration Management.
Design specifications have been verified against the formal top-level specification. Is incorrect because this would fall under Specification and verification.
References:
AIOv3 Security Models and Architecture (pages 302 - 306)
DOD TCSEC - http://www.cerberussystems.com/INFOSEC/stds/d520028.htm

NEW QUESTION: 496
CORRECT TEXT
Trend Analysis involves analyzing historical _____ files in order to look for patterns of abuse or misuse.
Answer:
files

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam!
BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here:
https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps,
40%OFF Special Discount: Exam-Tests)

NEW QUESTION: 497
Which type of firewall can be used to track connectionless protocols such as UDP and RPC?
A. Stateful inspection firewalls
B. Packet filtering firewalls
C. Application level firewalls
D. Circuit level firewalls
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Packets in a stateful inspection firewall are queued and then analyzed at all OSI layers, providing a more complete inspection of the data. By examining the state and context of the incoming data packets, it helps

to track the protocols that are considered "connectionless", such as UDP-based applications and Remote Procedure Calls (RPC).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
91).

NEW QUESTION: 498
The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?
A. clipping level
B. acceptance level
C. forgiveness level
D. logging level
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The correct answer is "clipping level". This is the point at which a system decides to take some sort of action when an action repeats a preset number of times. That action may be to log the activity, lock a user account, temporarily close a port, etc.
Example: The most classic example of a clipping level is failed login attempts. If you have a system configured to lock a user's account after three failed login attemts, that is the "clipping level".
The other answers are not correct because:
Acceptance level, forgiveness level, and logging level are nonsensical terms that do not exist (to my knowledge) within network security.
Reference:
Official ISC2 Guide - The term "clipping level" is not in the glossary or index of that book. I cannot find it in the text either. However, I'm quite certain that it would be considered part of the CBK, despite its exclusion from the Official Guide.
All in One Third Edition page: 136 - 137

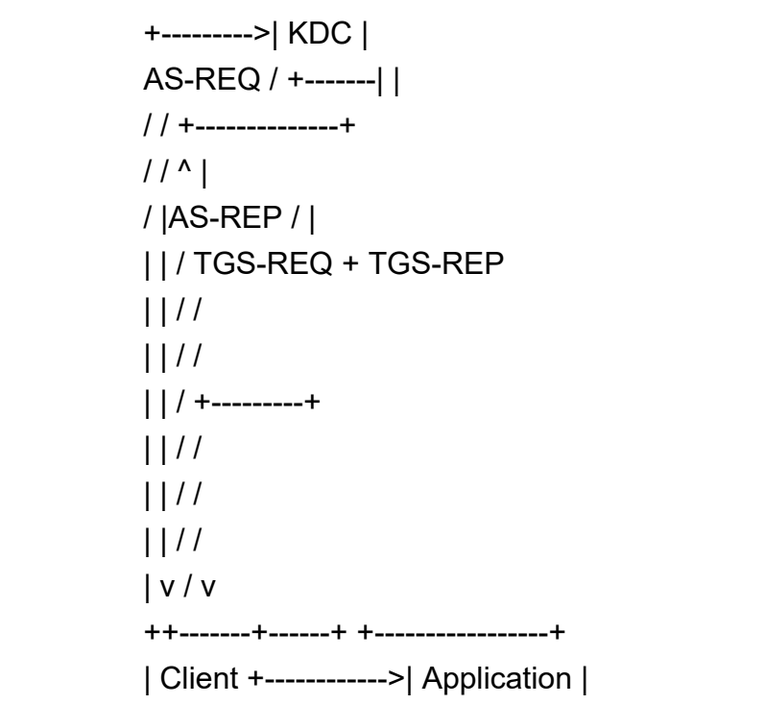
NEW QUESTION: 499
Related to information security, confidentiality is the opposite of which of the following?
A. closure
B. disclosure
C. disposal
D. disaster
Answer: B (LEAVE A REPLY)
Confidentiality is the opposite of disclosure.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 500
The Computer Security Policy Model the Orange Book is based on is which of the following?
A. Bell-LaPadula
B. Data Encryption Standard
C. Kerberos
D. Tempest
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The Computer Security Policy Model Orange Book is based is the Bell-LaPadula Model. Orange Book Glossary.
The Data Encryption Standard (DES) is a cryptographic algorithm. National Information Security Glossary.
TEMPEST is related to limiting the electromagnetic emanations from electronic equipment.
Reference: U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28-STD. December 1985 (also available here).

NEW QUESTION: 501
Select three ways to deal with risk.
A. Acceptance
B. Transfer
C. Deny
D. Mitigate
E. Avoid / Eliminate
Answer: (SHOW ANSWER)

NEW QUESTION: 502
Which of the following statements pertaining to using Kerberos without any extension is false?
A. A client can be impersonated by password-guessing.
B. Kerberos is mostly a third-party authentication protocol.
C. Kerberos uses public key cryptography.
D. Kerberos provides robust authentication.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Kerberos is a trusted, credential-based, third-party authentication protocol that uses symmetric (secret) key cryptography to provide robust authentication to clients accessing services on a network.
Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.
Here is a nice overview of HOW Kerberos is implement as described in RFC 4556:
1. Introduction
The Kerberos V5 protocol [RFC4120] involves use of a trusted third party known as the Key Distribution Center (KDC) to negotiate shared

session keys between clients and services and provide mutual authentication between them.
The corner-stones of Kerberos V5 are the Ticket and the Authenticator. A Ticket encapsulates a symmetric key (the ticket session key) in an envelope (a public message) intended for a specific service. The contents of the Ticket are encrypted with a symmetric key shared between the service principal and the issuing KDC. The encrypted part of the Ticket contains the client principal name, among other items. An Authenticator is a record that can be shown to have been recently generated using the ticket session key in the associated Ticket. The ticket session key is known by the client who requested the ticket. The contents of the Authenticator are encrypted with the associated ticket session key. The encrypted part of an Authenticator contains a timestamp and the client principal name, among other items.
As shown in Figure 1, below, the Kerberos V5 protocol consists of the following message exchanges between the client and the KDC, and the
client and the application service:
The Authentication Service (AS) Exchange
The client obtains an "initial" ticket from the Kerberos authentication server (AS), typically a Ticket Granting Ticket (TGT). The AS-REQ message and the AS-REP message are the request and the reply message, respectively, between the client and the AS.
The Ticket Granting Service (TGS) Exchange
The client subsequently uses the TGT to authenticate and request a service ticket for a particular service, from the Kerberos ticket-granting server (TGS). The TGS-REQ message and the TGS-REP message are the request and the reply message respectively between the client and the TGS.
The Client/Server Authentication Protocol (AP) Exchange
The client then makes a request with an AP-REQ message, consisting of a service ticket and an authenticator that certifies the client's possession of the ticket session key. The server may optionally reply with an AP-REP message. AP exchanges typically negotiate session-specific symmetric keys.
Usually, the AS and TGS are integrated in a single device also known as the KDC.



| | AP-REQ | Server |
| |<------------| |
+---------------+ AP-REP +-----------------+
Figure 1: The Message Exchanges in the Kerberos V5 Protocol
In the AS exchange, the KDC reply contains the ticket session key, among other items, that is encrypted using a key (the AS reply key)
shared between the client and the KDC. The AS reply key is typically derived from the client's password for human users. Therefore, for
human users, the attack resistance strength of the Kerberos protocol is no stronger than the strength of their passwords.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 40).
And
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 147-151).
and
http://www.ietf.org/rfc/rfc4556.txt

NEW QUESTION: 503
All following observations about IPSec are correct except:
A. Default Hashing protocols are HMAC-MD5 or HMAC-SHA-1
B. Default Encryption protocol is Cipher Block Chaining mode DES, but other algorithms like ECC (Elliptic curve cryptosystem) can be used
C. Support two communication modes - Tunnel mode and Transport mode
D. Works only with Secret Key Cryptography
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Pages 166-167.

NEW QUESTION: 504
Which of the following protocols does not operate at the data link layer (layer 2)?
A. PPP
B. RARP
C. L2F
D. ICMP
Answer: (SHOW ANSWER)
Explanation/Reference:
ICMP is the only of the mentioned protocols to operate at the network layer (layer 3). Other protocols operate at layer 2.

Source: WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April
2002 (page 1).

NEW QUESTION: 505
Upon which of the following ISO/OSI layers does network address translation operate?
A. Transport layer
B. Session layer
C. Data link layer
D. Network layer
Answer: (SHOW ANSWER)
Network address translation (NAT) is concerned with IP address translation
between two networks and operates at the network layer (layer 3).
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-
Hill/Osborne, 2002, Chapter 3: Telecommunications and Network Security (page 440).

NEW QUESTION: 506
In SSL/TLS protocol, what kind of authentication is supported when you establish a secure session between a client and a server?
A. Peer-to-peer authentication
B. Only server authentication (optional)
C. Server authentication (mandatory) and client authentication (optional)
D. Role based authentication scheme
Answer: C (LEAVE A REPLY)
Explanation/Reference:
RESCORLA, Eric, SSL and TLS: Designing and Building Secure Systems, 2000, Addison Wesley Professional; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

NEW QUESTION: 507
The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system is referred to as?
A. Confidentiality
B. Availability
C. Integrity
D. Reliability
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
An company security program must:
1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability;

2) protect informationcommensurate with the level of risk and magnitude ofharmresulting fromloss, misuse, unauthorized access, or modification.
The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.
The following are incorrect answers:
Confidentiality - The information requires protection from unauthorized disclosure and only the INTENDED recipient should have access to the meaning of the data either in storage or in transit.
Integrity - The information must be protected from unauthorized, unanticipated, or unintentional modification.
This includes, but is not limited to:
Authenticity -A third party must be able to verify that the content of a message has not been changed in transit.
Non-repudiation - The origin or the receipt of a specific message must be verifiable by a third party.
Accountability - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
Reference used for this question:
RFC 2828
and
SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (page 5).

NEW QUESTION: 508
What would BEST define risk management?
A. The process of eliminating the risk
B. The process of assessing the risks
C. The process of reducing risk to an acceptable level
D. The process of transferring risk
Answer: C (LEAVE A REPLY)
Explanation/Reference:
This is the basic process of risk management.
Risk is the possibility of damage happening and the ramifications of such damage should it occur. Information risk management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.
Proper risk management requires a strong commitment from senior management, a documented process that supports the organization's mission, an information risk management (IRM) policy and a delegated

IRM team. Once you've identified your company's acceptable level of risk, you need to develop an information risk management policy.

The IRM policy should be a subset of the organization's overall risk management policy (risks to a company include more than just information security issues) and should be mapped to the organizational security policies, which lay out the acceptable risk and the role of security as a whole in the organization. The IRM policy is focused on risk management while the security policy is very high-level and addresses all aspects of security. The IRM policy should address the following items:

Objectives of IRM team

Level of risk the company will accept and what is considered an acceptable risk (as defined in the previous article)

Formal processes of risk identification

Connection between the IRM policy and the organization's strategic planning processes Responsibilities that fall under IRM and the roles that are to fulfill them Mapping of risk to internal controls

Approach for changing staff behaviors and resource allocation in response to risk analysis Mapping of risks to performance targets and budgets

Key indicators to monitor the effectiveness of controls

Shon Harris provides a 10,000-foot view of the risk management process below:

A big question that companies have to deal with is, "What is enough security?" This can be restated as, "What is our acceptable risk level?" These two questions have an inverse relationship. You can't know what constitutes enough security unless you know your necessary baseline risk level.

To set an enterprise-wide acceptable risk level for a company, a few things need to be investigated and understood. A company must understand its federal and state legal requirements, its regulatory requirements, its business drivers and objectives, and it must carry out a risk and threat analysis. (I will dig deeper into formalized risk analysis processes in a later article, but for now we will take a broad approach.) The result of these findings is then used to define the company's acceptable risk level, which is then outlined in security policies, standards, guidelines and procedures.

Although there are different methodologies for enterprise risk management, the core components of any risk analysis is made up of the following:

Identify company assets

Assign a value to each asset

Identify each asset's vulnerabilities and associated threats

Calculate the risk for the identified assets

Once these steps are finished, then the risk analysis team can identify the necessary countermeasures to mitigate the calculated risks, carry out cost/benefit analysis for these countermeasures and report to senior management their findings.

When we look at information security, there are several types of risk a corporation needs to be aware of and address properly. The following items touch on the major categories:

Physical damage Fire, water, vandalism, power loss, and natural disasters Human interaction Accidental or intentional action or inaction that can disrupt productivity Equipment malfunction Failure of systems and peripheral devices

Inside and outside attacks Hacking, cracking, and attacking

Misuse of data Sharing trade secrets, fraud, espionage, and theft
Loss of data Intentional or unintentional loss of information through destructive means Application error Computation errors, input errors, and buffer overflows The following answers are incorrect:
The process of eliminating the risk is not the best answer as risk cannot be totally eliminated.
The process of assessing the risks is also not the best answer.
The process of transferring risk is also not the best answer and is one of the ways of handling a risk after a risk analysis has been performed.
References:
Shon Harris , AIO v3 , Chapter 3: Security Management Practices , Page: 66-68 and http://searchsecurity.techtarget.com/tip/Understanding-risk

NEW QUESTION: 509
Whose role is it to assign classification level to information?
A. Security Administrator
B. User
C. Owner
D. Auditor
Answer: C (LEAVE A REPLY)
Explanation/Reference:
The Data/Information Owner is ultimately responsible for the protection of the data. It is the Data/ Information Owner that decides upon the classifications of that data they are responsible for.
The data owner decides upon the classification of the data he is responsible for and alters that classification if the business need arises.
The following answers are incorrect:
Security Administrator. Is incorrect because this individual is responsible for ensuring that the access right granted are correct and support the polices and directives that the Data/Information Owner defines.
User. Is Incorrect because the user uses/access the data according to how the Data/Information Owner defined their access.
Auditor. Is incorrect because the Auditor is responsible for ensuring that the access levels are appropriate.
The Auditor would verify that the Owner classified the data properly.
References:
CISSP All In One Third Edition, Shon Harris, Page 121

NEW QUESTION: 510
Which of the following services relies on UDP?
A. FTP
B. Telnet
C. DNS
D. SMTP
Answer: C (LEAVE A REPLY)

Explanation/Reference:
DNS relies on connectionless UDP whereas services like FTP, Telnet and SMTP rely on TCP.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

NEW QUESTION: 511
Which of the following is a large hardware/software backup system that uses the RAID technology?
A. Tape Array.
B. Scale Array.
C. Crimson Array
D. Table Array.
Answer: A (LEAVE A REPLY)
A Tape Array is a large hardware/software backup system based on the
RAID technology.
There is a misconception that RAID can only be used with Disks.
All large storage vendor from HP, to EMC, to Compaq have Tape Array based on RAID technology they offer.
This is a VERY common type of storage at an affordable price as well.
So RAID is not exclusively for DISKS. Often time this is referred to as Tape Librairies or simply RAIT.
RAIT (redundant array of independent tapes) is similar to RAID, but uses tape drives instead of disk drives. Tape storage is the lowest-cost option for very large amounts of data, but is very slow compared to disk storage. As in RAID 1 striping, in RAIT, data are striped in parallel to multiple tape drives, with or without a redundant parity drive. This provides the high capacity at low cost typical of tape storage, with higher-than-usual tape data transfer rates and optional data integrity.
References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 70. and Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1271). McGraw-Hill. Kindle Edition.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 512

What security problem is most likely to exist if an operating system permits objects to be used sequentially by multiple users without forcing a refresh of the objects?
A. Disclosure of residual data.
B. Unauthorized obtaining of a privileged execution state.
C. Denial of service through a deadly embrace.
D. Data leakage through covert channels.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
This question is asking you to consider the effects of object reuse. Object reuse is "reassigning to subject media that previously contained information. Object reuse is a security concern because if insufficient measures were taken to erase the information on the media, the information may be disclosed to unauthorized personnel." This concept relates to Security Architecture and Design, because it is in level C2: Controlled Access Protection, of the Orange Book, where "The object reuse concept must be invoked, meaning that any medium holding data must not contain any remnants of information after it is release for another subject to use." REFERENCE:
AIO Version 5 (Shon Harris), page 360
and
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 513
TCPWrappers is an example of which type of security tool?
A. All of the above
B. Host Based IDS
C. Personal Firewall
D. Network Based IDS
E. None of the above
Answer: B (LEAVE A REPLY)

NEW QUESTION: 514
Which type of algorithm is considered to have the highest strength per bit of key length of any of the asymmetric algorithms?
A. Rivest, Shamir, Adleman (RSA)
B. El Gamal
C. Elliptic Curve Cryptography (ECC)
D. Advanced Encryption Standard (AES)
Answer: C (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
The other answers are not correct because:

"Rivest, Shamir, Adleman (RSA)" is incorrect because RSA is a "traditional" asymmetric algorithm. While it is reasonably strong, it is not considered to be as strong as ECC based systems.
"El Gamal" is incorrect because it is also a "traditional" asymmetric algorithm and not considered as strong as ECC based systems.
"Advanced Encryption Standard (AES)" is incorrect because the question asks specifically about asymmetric algorithms and AES is a symmetric algorithm.
References:
Official ISC2 Guide page: 258
All in One Third Edition page: 638
The RSA Crypto FAQ: http://www.rsa.com/rsalabs/node.asp?id=2241

NEW QUESTION: 515
IPSEC resides at which layer of the OSI model?
A. Layer 3 - Network
B. Layer 6 - Presentation
C. Layer 2 - Data Link
D. Layer 1 - Physical
E. Layer 5 - Session
F. Layer 4 - Transport
Answer: A (LEAVE A REPLY)

NEW QUESTION: 516
Which of the following is a disadvantage of a statistical anomaly-based intrusion detection system?
A. it may truly detect a non-attack event that had caused a momentary anomaly in the system.
B. it may falsely detect a non-attack event that had caused a momentary anomaly in the system.
C. it may correctly detect a non-attack event that had caused a momentary anomaly in the system.
D. it may loosely detect a non-attack event that had caused a momentary anomaly in the system.
Answer: (SHOW ANSWER)
Section: Analysis and Monitoring
Explanation/Reference:
Some disadvantages of a statistical anomaly-based ID are that it will not detect an attack that does not significantly change the system operating characteristics, or it may falsely detect a non-attack event that had caused a momentary anomaly in the system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

NEW QUESTION: 517
What is the maximum key size for the RC5 algorithm?
A. 128 bits
B. 256 bits
C. 1024 bits

D. 2040 bits

Answer: D (LEAVE A REPLY)

RC5 is a fast block cipher created by Ron Rivest and analyzed by RSA Data Security, Inc.
It is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds.
Allowable choices for the block size are 32 bits (for experimentation and evaluation purposes only), 64 bits (for use a drop-in replacement for DES), and 128 bits.
The number of rounds can range from 0 to 255, while the key can range from 0 bits to 2040 bits in size.
Please note that some sources such as the latest Shon Harris book mentions that RC5 maximum key size is of 2048, not 2040 bits. I would definitively use RSA as the authoritative source which specifies a key of 2040 bits. It is an error in Shon's book.
The OIG book says: RC5 was developed by Ron Rivest of RSA and is deployed in many of RSA's products. It is a very adaptable product useful for many applications, ranging from software to hardware implementations. The key for RC5 can vary from 0 to 2040 bits, the number of rounds it executes can be adjusted from 0 to 255, and the length of the input words can also be chosen from 16-, 32-, and 64-bit lengths.
The following answers were incorrect choices:
All of the other answers were wrong.
Reference(s) used for this question:
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Cryptography (Kindle Locations 1098-1101). . Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 16744-16747). McGraw-Hill. Kindle Edition. http://www.rsa.com/rsalabs/node.asp?id=2251, What are RC5 and RC6, RSA The Security Division of EMC. From Rivest himself, see http://people.csail.mit.edu/rivest/Rivest-rc5rev.pdf Also see the draft IETF IPSEC standard which clearly mention that it is in fact 2040 bits as a MAXIMUM key size: http://www.tools.ietf.org/html/draft-ietf-ipsec-esp-rc5-cbc-00 http://en.wikipedia.org/wiki/RC5, Mention a maximum key size of 2040 as well.

NEW QUESTION: 518

What can be defined as a momentary low voltage?

A. Spike

B. Sag

C. Fault

D. Brownout

Answer: (SHOW ANSWER)

A sag is a momentary low voltage. A spike is a momentary high voltage. A fault is a momentary power out and a brownout is a prolonged power supply that is below normal voltage. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 6: Physical security (page 299)

NEW QUESTION: 519

The criteria for evaluating the legal requirements for implementing safeguards is to evaluate the cost (C) of instituting the protection versus the estimated loss (L) resulting from the exploitation of the corresponding vulnerability. Therefore, a legal liability may exists when:

A. (C < L) or C is less than L

B. (C < L - (residual risk)) or C is less than L minus residual risk

C. (C > L) or C is greather than L

D. (C > L - (residual risk)) or C is greather than L minus residual risk

Answer: (SHOW ANSWER)

Explanation/Reference:

If the cost is lower than the estimated loss (C < L), then legal liability may exists if you fail to implement the proper safeguards.

Government laws and regulations require companies to employ reasonable security measures to reduce private harms such as identity theft due to unauthorized access. The U.S. Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and the broader European Directive 95/46/EC, Article 17, both require that companies employ reasonable or

appropriate administrative and technical security measures to protect consumer information.

The GLBA is a U.S. Federal law enacted by U.S. Congress in 1998 to allow consolidation among commercial banks. The GLBA Safeguards Rule is U.S. Federal regulation created in reaction to the GLBA and enforced by the U.S.

Federal Trade Commission (FTC). The Safeguards Rule requires companies to implement a security plan to protect the confidentiality and integrity of consumer personal information and requires the designation of an individual responsible for compliance.

Because these laws and regulations govern consumer personal information, they can lead to new requirements for information systems for which companies are responsible to comply.

The act of compliance includes demonstrating due diligence, which is defined as "reasonable efforts that persons make to satisfy legal requirements or discharge their legal obligations". Reasonableness in software systems includes industries standards and may allow for imperfection. Lawyers representing firms and other organizations, regulators, system administrators and engineers all face considerable challenge in determining what constitutes "reasonable" security measures for several reasons, including:

1. Compliance changes with the emergence of new security vulnerabilities due to innovations in information technology;

2. Compliance requires knowledge of specific security measures, however publicly available best practices typically include general goals and only address broad categories of vulnerability; and

3. Compliance is a best-effort practice, because improving security is costly and companies must prioritize security spending commensurate with risk of non-compliance. In general, the costs of improved security are certain, but the

improvement in security depends on unknown variables and probabilities outside the control of companies.

The following reference(s) were used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 315.

and
http://www.cs.cmu.edu/~breaux/publications/tdbreaux-cose10.pdf

NEW QUESTION: 520
Which of the following best describes signature-based detection?
A. Compare source code, looking for events or sets of events that could cause damage to a system or network.
B. Compare system activity for the behaviour patterns of new attacks.
C. Compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack.
D. Compare network nodes looking for objects or sets of objects that match a predefined pattern of objects that may describe a known attack.
Answer: C (LEAVE A REPLY)
Section: Analysis and Monitoring
Explanation/Reference:
Misuse detectors compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called "signature-based detection." The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. However, there are more sophisticated approaches to doing misuse detection (called "state-based" analysis techniques) that can leverage a single signature to detect groups of attacks.
Reference:
Old Document:
BACE, Rebecca & MELL, Peter, NIST Special Publication 800-31 on Intrusion Detection Systems, Page 16.
The publication above has been replaced by 800-94 on page 2-4
The Updated URL is: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

NEW QUESTION: 521
Which of the following would assist the most in Host Based intrusion detection?
A. audit trails.
B. access control lists.
C. security clearances.
D. host-based authentication.
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
To assist in Intrusion Detection you would review audit logs for access violations.
The following answers are incorrect:

access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.
security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.
host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not dectect intrusions.

NEW QUESTION: 522
The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers does NOT have which of the following characteristics?
A. Standard model for network communications
B. Used to gain information from network devices such as count of packets received and routing tables
C. Enables dissimilar networks to communicate
D. Defines 7 protocol layers (a.k.a. protocol stack)
Answer: (SHOW ANSWER)
The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers and Characteristics Standard model for network communications enables dissimilar networks to communicate, Defines 7 protocol layers (a.k.a. protocol stack) Each layer on one workstation communicates with its respective layer on another workstation using protocols (i.e. agreed-upon communication formats) "Mapping" each protocol to the model is useful for comparing protocols.
Mnemonics: Please Do Not Throw Sausage Pizza Away (bottom to top layer)
All People Seem To Need Data Processing (top to bottom layer).
Source: STEINER, Kurt, Telecommunications and Network Security, Version 1, May 2002, CISSP Open Study Group (Domain Leader: skottikus), Page 12.

NEW QUESTION: 523
Which of the following is NOT a common backup method?
A. Full backup method
B. Daily backup method
C. Incremental backup method
D. Differential backup method
Answer: B (LEAVE A REPLY)
A daily backup is not a backup method, but defines periodicity at which backups are made. There can be daily full, incremental or differential backups. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).

NEW QUESTION: 524
Which of the following statements pertaining to biometrics is FALSE?
A. User can be authenticated based on behavior.

B. User can be authenticated based on unique physical attributes.
C. User can be authenticated by what he knows.
D. A biometric system's accuracy is determined by its crossover error rate (CER).
Answer: C (LEAVE A REPLY)
Explanation/Reference:
As this is not a characteristic of Biometrics this is the rigth choice for this question. This is one of the three basic way authentication can be performed and it is not related to Biometrics. Example of something you know would be a password or PIN for example.
Please make a note of the negative 'FALSE' within the question. This question may seem tricky to some of you but you would be amazed at how many people cannot deal with negative questions. There will be a few negative questions within the real exam, just like this one the keyword NOT or FALSE will be in Uppercase to clearly indicate that it is negative.
Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of performing authentication (one to one matching) or identification (a one to many matching).
A biometric system scans an attribute or behavior of a person and compares it to a template store within an authentication server datbase, such template would be created in an earlier enrollment process.
Because this system inspects the grooves of a person's fingerprint, the pattern of someone's retina, or the pitches of someone's voice, it has to be extremely sensitive.
The system must perform accurate and repeatable measurements of anatomical or physiological characteristics. This type of sensitivity can easily cause false positives or false negatives. The system must be calibrated so that these false positives and false negatives occur infrequently and the results are as accurate as possible.
There are two types of failures in biometric identification:
False Rejection also called False Rejection Rate (FRR) - The system fail to recognize a legitimate user. While it could be argued that this has the effect of keeping the protected area extra secure, it is an intolerable frustration to legitimate users who are refused access because the scanner does not recognize them.
False Acceptance or False Acceptance Rate (FAR) - This is an erroneous recognition, either by confusing one user with another or by accepting an imposter as a legitimate user.
Physiological Examples:
Unique Physical Attributes:
Fingerprint (Most commonly accepted)
Hand Geometry
Retina Scan (Most accurate but most intrusive)
Iris Scan
Vascular Scan
Behavioral Examples:
Repeated Actions
Keystroke Dynamics

(Dwell time (the time a key is pressed) and Flight time (the time between "key up" and the next "key down").
Signature Dynamics
(Stroke and pressure points)
EXAM TIP:
Retina scan devices are the most accurate but also the most invasive biometrics system available today. The continuity of the retinal pattern throughout life and the difficulty in fooling such a device also make it a great long-term, high-security option. Unfortunately, the cost of the proprietary hardware as well the stigma of users thinking it is potentially harmful to the eye makes retinal scanning a bad fit for most situations.
Remember for the exam that fingerprints are the most commonly accepted type of biometrics system.
The other answers are incorrect:
'Users can be authenticated based on behavior.' is incorrect as this choice is TRUE as it pertains to BIOMETRICS.
Biometrics systems makes use of unique physical characteristics or behavior of users.
'User can be authenticated based on unique physical attributes.' is also incorrect as this choice is also TRUE as it pertains to BIOMETRICS. Biometrics systems makes use of unique physical characteristics or behavior of users.
'A biometric system's accuracy is determined by its crossover error rate (CER)' is also incorrect as this is TRUE as it also pertains to BIOMETRICS. The CER is the point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of the CER, the more accurate the system.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25353-25356). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25297-25303). Auerbach Publications. Kindle Edition.

NEW QUESTION: 525
Which security model uses division of operations into different parts and requires different users to perform each part?
A. Bell-LaPadula model
B. Biba model
C. Clark-Wilson model
D. Non-interference model
Answer: C (LEAVE A REPLY)
The Clark-Wilson model uses separation of duties, which divides an
operation into different parts and requires different users to perform each part. This
prevents authorized users from making unauthorized modifications to data, thereby
protecting its integrity.
The Clark-Wilson integrity model provides a foundation for specifying and analyzing an

integrity policy for a computing system.
The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules.
The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction.
A well-formed transaction is a series of operations that transition a system from one consistent state to another consistent state.
In this model the integrity policy addresses the integrity of the transactions.
The principle of separation of duty requires that the certifier of a transaction and the implementer be different entities.
The model contains a number of basic constructs that represent both data items and processes that operate on those data items. The key data type in the Clark-Wilson model is a Constrained Data Item (CDI). An Integrity Verification Procedure (IVP) ensures that all CDIs in the system are valid at a certain state. Transactions that enforce the integrity policy are represented by Transformation Procedures (TPs). A TP takes as input a CDI or Unconstrained Data Item (UDI) and produces a CDI. A TP must transition the system from one valid state to another valid state. UDIs represent system input (such as that provided by a user or adversary). A TP must guarantee (via certification) that it transforms all possible values of a UDI to a "safe" CDI.
In general, preservation of data integrity has three goals:
Prevent data modification by unauthorized parties
Prevent unauthorized data modification by authorized parties
Maintain internal and external consistency (i.e. data reflects the real world)
Clark-Wilson addresses all three rules but BIBA addresses only the first rule of intergrity.
References:
HARRIS, Shon, All-In-One CISSP Certification Fifth Edition, McGraw-Hill/Osborne, Chapter 5: Security Architecture and Design (Page 341-344). and http://en.wikipedia.org/wiki/Clark-Wilson_model

NEW QUESTION: 526
Which of the following access control models introduces user security clearance and data classification?
A. Role-based access control
B. Discretionary access control
C. Non-discretionary access control
D. Mandatory access control
Answer: (SHOW ANSWER)
Section: Access Control

Explanation/Reference:
The mandatory access control model is based on a security label system. Users are given a security clearance and data is classified. The classification is stored in the security labels of the resources. Classification labels specify the level of trust a user must have to access a certain file.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4:
Access Control (Page 154).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 527
Compared to RSA, which of the following is true of Elliptic Curve Cryptography(ECC)?
A. It has been mathematically proved to be more secure.
B. It has been mathematically proved to be less secure.
C. It is believed to require longer key for equivalent security.
D. It is believed to require shorter keys for equivalent security.
Answer: (SHOW ANSWER)
Explanation/Reference:
The following answers are incorrect: It has been mathematically proved to be less secure. ECC has not been proved to be more or less secure than RSA. Since ECC is newer than RSA, it is considered riskier by some, but that is just a general assessment, not based on mathematical arguments.
It has been mathematically proved to be more secure. ECC has not been proved to be more or less secure than RSA. Since ECC is newer than RSA, it is considered riskier by some, but that is just a general assessment, not based on mathematical arguments.
It is believed to require longer key for equivalent security. On the contrary, it is believed to require shorter keys for equivalent security of RSA.
Shon Harris, AIO v5 pg719 states:
"In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter that what RSA requires" The following reference(s) were/was used to create this question:
ISC2 OIG, 2007 p. 258
Shon Harris, AIO v5 pg719

NEW QUESTION: 528

You are running a packet sniffer on a network and see a packet containing a long string of "0x90 0x90 0x90 0x90...." in the middle of it traveling to an x86-based machine as a target. This could be indicative of what activity being attempted?

A. Over-subscription of the traffic on a backbone.

B. A source quench packet.

C. A FIN scan.

D. A buffer overflow attack.

Answer: (SHOW ANSWER)

A series of the same control characters, hexadecimal code, imbedded in the string is usually an indicator of a buffer overflow attack.

The Intel x86 processors use the hexadecimal number 90 to represent NOP (no operation). Many buffer overflow attacks use long strings of control characters and this is representative of that type of attack.

A buffer overflow takes place when too much data are accepted as input to a specific process. A buffer is an allocated segment of memory. A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by commands the attacker wants executed. So, the purpose of a buffer overflow may be either to make a mess, by shoving arbitrary data into various memory segments, or to accomplish a specific task, by pushing into the memory segment a carefully crafted set of data that will accomplish a specific task. This task could be to open a command shell with administrative privilege or execute malicious code.

Common threats to system availability, integrity, and confidentiality include hardware failure, misuse of system privileges, buffer overflows and other memory attacks, denial of service, reverse engineering, and system hacking.

Since many vulnerabilities result from insecure design and most threats are well known, it is the responsibility of the security architect to ensure that their designs are addressing security requirements appropriately while also ensuring that the system can continue to perform its intended function.

The following answers are incorrect:

Over-subscription of the traffic on a backbone. Is incorrect because if there was Over-subscription of the traffic on a backbone, that would typically result in not being able to send or receive any packets, more commonly known as Denial of Service or DoS.

A source quench packet. This is incorrect because a source quench packet is an ICMP message that contains the internet header plus 64 bits of the original datagram.

A FIN scan. This is incorrect because a FIN scan is when a packet with the FIN flag set is sent to a specific port and the results are then analyzed.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Security Architecture and Design, Page 332, for people using the Kindle edition you will find it at Kindle Locations 7310-7315.

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Architecture and Design (Kindle Locations 1403-1407). . Kindle Edition.
Wikipedia http://en.wikipedia.org/wiki/Port_scanner
ICMP http://security.maruhn.com/iptables-tutorial/x1078.html
Wikipedia http://en.wikipedia.org/wiki/Buffer_overflow

NEW QUESTION: 529
Which of the following is less likely to be included in the change control sub-phase of the maintenance phase of a software product?
A. Estimating the cost of the changes requested
B. Recreating and analyzing the problem
C. Determining the interface that is presented to the user
D. Establishing the priorities of requests
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Change control sub-phase includes Recreating and analyzing the problem, Determining the interface that is presented to the user, and Establishing the priorities of requests.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).

NEW QUESTION: 530
Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?
A. Degaussing
B. Parity Bit Manipulation
C. Zeroization
D. Buffer overflow
Answer: A (LEAVE A REPLY)
Explanation/Reference:
A "Degausser (Otherwise known as a Bulk Eraser) has the main function of reducing to near zero the magnetic flux stored in the magnetized medium. Flux density is measured in Gauss or Tesla. The operation is speedier than overwriting and done in one short operation. This is achieved by subjecting the subject in bulk to a series of fields of alternating polarity and gradually decreasing strength.
The following answers are incorrect:Parity Bit Manipulation. Parity has to do with disk lerror detection, not data removal. A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the infromation that was sent.
Zeroization. Zeroization involves overwrting data to sanitize it. It is time-consuming and not foolproof. The potential of restoration of data does exist with this method.
Buffer overflow. This is a detractor. Although many Operating Systems use a disk buffer to temporarily hold data read from disk, its primary purpose has no connection to data removal. An overflow goes

outside the constraints defined for the buffer and is a method used by an attacker to attempt access to a system.
The following reference(s) were/was used to create this question:
Shon Harris AIO v3. pg 908
Reference: What is degaussing.

NEW QUESTION: 531
What are the components of an object's sensitivity label?
A. A Classification Set and a single Compartment.
B. A single classification and a single compartment.
C. A Classification Set and user credentials.
D. A single classification and a Compartment Set.
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Both are the components of a sensitivity label.
The following are incorrect:
A Classification Set and a single Compartment. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classifcation and it is not a "single compartment" but a Compartment Set.
A single classification and a single compartment. Is incorrect because while there only is one classifcation, it is not a "single compartment" but a Compartment Set.
A Classification Set and user credentials. Is incorrect because the nomenclature "Classification Set" is incorrect, there only one classifcation and it is not "user credential" but a Compartment Set. The user would have their own sensitivity label.

NEW QUESTION: 532
Which of the following is responsible for MOST of the security issues?
A. Outside espionage
B. Hackers
C. Personnel
D. Equipment failure
Answer: (SHOW ANSWER)
Personnel cause more security issues than hacker attacks, outside
espionage, or equipment failure.
The following answers are incorrect because:
Outside espionage is incorrect as it is not the best answer.
Hackers is also incorrect as it is not the best answer.
Equipment failure is also incorrect as it is not the best answer.
Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 56

NEW QUESTION: 533

In biometric identification systems, the parts of the body conveniently available for identification are:
A. neck and mouth
B. hands, face, and eyes
C. feet and hair
D. voice and neck
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Today implementation of fast, accurate, reliable, and user-acceptable biometric identification systems are already under way. Because most identity authentication takes place when a people are fully clothed (neck to feet and wrists), the parts of the body conveniently available for this purpose are hands, face, and eyes.
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

NEW QUESTION: 534
Which of the following would best describe a Concealment cipher?
A. Permutation is used, meaning that letters are scrambled.
B. Every X number of words within a text, is a part of the real message.
C. Replaces bits, characters, or blocks of characters with different bits, characters or blocks.
D. Hiding data in another message so that the very existence of the data is concealed.
Answer: B (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
When a concealment cipher is used, every X number of words within a text, is a part of the real message. The message is within another message.
A concealment cipher is a message within a message. If my other super-secret spy buddy and I decide our key value is every third word, then when I get a message from him, I will pick out every third word and write it down.
Suppose he sends me a message that reads, "The saying, 'The time is right' is not cow language, so is now a dead subject." Because my key is every third word, I come up with "The right cow is dead." This again means nothing to me, and I am now turning in my decoder ring.
Concealment ciphers include the plaintext within the ciphertext. It is up to the recipient to know which letters or symbols to exclude from the ciphertext in order to yield the plaintext. Here is an example of a concealment cipher:
i2l32i5321k34e1245ch456oc12ol234at567e
Remove all the numbers, and you'll have i like chocolate. How about this one?
Larry even appears very excited. No one worries.
The first letter from each word reveals the message leave now. Both are easy, indeed, but many people have crafted more ingenious ways of concealing the messages. By the way, this type of cipher doesn't even need ciphertext, such as that in the above examples.

Consider the invisible drying ink that kids use to send secret messages. In a more extreme example, a man named Histiaeus, during 5th century B.C., shaved the head of a trusted slave, then tattooed the message onto his bald head. When the slave's hair grew back, Histiaeus sent the slave to the message's intended recipient, Aristagoros, who shaved the slave's head and read the message instructing him to revolt.
The following answers are incorrect:
A transposition cipher uses permutations.
A substitution cipher replaces bits, characters, or blocks of characters with different bits, characters or blocks.
Steganography refers to hiding the very existence of the message.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 1).
and also see:
http://www.go4expert.com/forums/showthread.php?t=415

NEW QUESTION: 535
Which type of attack involves impersonating a user or a system?
A. Smurfing attack
B. Spoofing attack
C. Spamming attack
D. Sniffing attack
Answer: B (LEAVE A REPLY)
A spoofing attack is when an attempt is made to gain access to a computer system by posing as an authorized user or system. Spamming refers to sending out or posting junk advertising and unsolicited mail. A smurf attack is a type of denial-of-service attack using PING and a spoofed address. Sniffing refers to observing packets passing on a network. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

NEW QUESTION: 536
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It does not permit management to:
A. specify what users can do
B. specify which resources they can access
C. specify how to restrain hackers
D. specify what operations they can perform on a system.
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to

specify what users can do, which resources they can access, and what operations they can perform on a system. Specifying HOW to restrain hackers is not directly linked to access control.
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 12.

NEW QUESTION: 537
What best describes a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account?
A. Data fiddling
B. Data diddling
C. Salami techniques
D. Trojan horses
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 644.

NEW QUESTION: 538
Overloading or congesting a system's resources so that it is unable to provide required services is referred to as:
A. Swamping
B. Denial of Service
C. Bandwidth displacement
D. A passive attack
E. ICMP redirect
Answer: B (LEAVE A REPLY)
A denial-of-service attack is aimed at depriving an organization of its resources. They are typically intentional attacks targeted against a specific system or network.

NEW QUESTION: 539
Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/software units. Such controls, also known as logical controls, represent which pairing?
A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Technical Pairing
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Preventive/Technical controls are also known as logical controls and can be built into the operating system, be software applications, or can be supplemental hardware/software units.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION: 540
Which of the following phases of a software development life cycle normally addresses Due Care and Due Diligence?
A. Implementation
B. System feasibility
C. Product design
D. Software plans and requirements
Answer: D (LEAVE A REPLY)
The software plans and requirements phase addresses threats, vulnerabilities, security requirements, reasonable care, due diligence, legal liabilities, cost/benefit analysis, level of protection desired, test plans.
Implementation is incorrect because it deals with Installing security software, running the system, acceptance testing, security software testing, and complete documentation certification and accreditation (where necessary).
System Feasibility is incorrect because it deals with information security policy, standards, legal issues, and the early validation of concepts.
Product design is incorrect because it deals with incorporating security specifications,
adjusting test plans and data,
determining access controls, design documentation, evaluating encryption options, and verification.
Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Security Life Cycle Components, Figure 7.5 (page 346).

NEW QUESTION: 541
Making sure that the data has not been changed unintentionally, due to an accident or malice is:
A. Integrity.
B. Confidentiality.
C. Availability.
D. Auditability.
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Integrity refers to the protection of information from unauthorized modification or deletion.

Confidentiality is incorrect. Confidentiality refers to the protection of information from unauthorized disclosure.
Availability is incorrect. Availability refers to the assurance that information and services will be available to authorized users in accordance with the service level objective.
Auditability is incorrect. Auditability refers to the ability to trace an action to the identity that performed it and identify the date and time at which it occurred.
References:
CBK, pp. 5 - 6
AIO3, pp. 56 - 57

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 542
Which of the following statements pertaining to biometrics is FALSE?
A. User can be authenticated based on behavior.
B. User can be authenticated based on unique physical attributes.
C. User can be authenticated by what he knows.
D. A biometric system's accuracy is determined by its crossover error rate (CER).
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
As this is not a characteristic of Biometrics this is the rigth choice for this question. This is one of the three basic way authentication can be performed and it is not related to Biometrics. Example of something you know would be a password or PIN for example.
Please make a note of the negative 'FALSE' within the question. This question may seem tricky to some of you but you would be amazed at how many people cannot deal with negative questions. There will be a few negative questions within the real exam, just like this one the keyword NOT or FALSE will be in Uppercase to clearly indicate that it is negative.
Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of performing authentication (one to one matching) or identification (a one to many matching).
A biometric system scans an attribute or behavior of a person and compares it to a template store within an authentication server datbase, such template would be created in an earlier enrollment process.

Because this system inspects the grooves of a person's fingerprint, the pattern of someone's retina, or the pitches of someone's voice, it has to be extremely sensitive.
The system must perform accurate and repeatable measurements of anatomical or physiological characteristics. This type of sensitivity can easily cause false positives or false negatives. The system must be calibrated so that these false positives and false negatives occur infrequently and the results are as accurate as possible.
There are two types of failures in biometric identification:
False Rejection also called False Rejection Rate (FRR) - The system fail to recognize a legitimate user. While it could be argued that this has the effect of keeping the protected area extra secure, it is an intolerable frustration to legitimate users who are refused access because the scanner does not recognize them.
False Acceptance or False Acceptance Rate (FAR) - This is an erroneous recognition, either by confusing one user with another or by accepting an imposter as a legitimate user.
Physiological Examples:
Unique Physical Attributes:
Fingerprint (Most commonly accepted)
Hand Geometry
Retina Scan (Most accurate but most intrusive)
Iris Scan
Vascular Scan
Behavioral Examples:
Repeated Actions
Keystroke Dynamics
(Dwell time (the time a key is pressed) and Flight time (the time between "key up" and the next "key down").
Signature Dynamics
(Stroke and pressure points)
EXAM TIP:
Retina scan devices are the most accurate but also the most invasive biometrics system available today. The continuity of the retinal pattern throughout life and the difficulty in fooling such a device also make it a great long-term, high-security option. Unfortunately, the cost of the proprietary hardware as well the stigma of users thinking it is potentially harmful to the eye makes retinal scanning a bad fit for most situations.
Remember for the exam that fingerprints are the most commonly accepted type of biometrics system.
The other answers are incorrect:
'Users can be authenticated based on behavior.' is incorrect as this choice is TRUE as it pertains to BIOMETRICS.
Biometrics systems makes use of unique physical characteristics or behavior of users.
'User can be authenticated based on unique physical attributes.' is also incorrect as this choice is also TRUE as it pertains to BIOMETRICS. Biometrics systems makes use of unique physical characteristics or behavior of users.

'A biometric system's accuracy is determined by its crossover error rate (CER)' is also incorrect as this is TRUE as it also pertains to BIOMETRICS. The CER is the point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of the CER, the more accurate the system.
Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25353-25356). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25297-25303). Auerbach Publications. Kindle Edition.

NEW QUESTION: 543
In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?
A. Both client and server
B. The client's browser
C. The web server
D. The merchant's Certificate Server
Answer: B (LEAVE A REPLY)
Once the merchant server has been authenticated by the browser client, the browser generates a master secret that is to be shared only between the server and client. This secret serves as a seed to generate the session (private) keys. The master secret is then encrypted with the merchant's public key and sent to the server. The fact that the master secret is generated by the client's browser provides the client assurance that the server is not reusing keys that would have been used in a previous session with another client.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 112).
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, page 569.

NEW QUESTION: 544
Which of the following are REGISTERED PORTS as defined by IANA ?
A. Ports 128 to 255
B. Ports 1024 to 49151
C. Ports 1025 to 65535
D. Ports 1024 to 32767
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Ports 1024 to 49151 has been defined as REGISTERED PORTS by IANA.
A registered port is a network port (a sub-address defined within the Internet Protocol, in the range 1-

65535) assigned by the Internet Assigned Numbers Authority (IANA) (or by Internet Corporation for Assigned Names and Numbers (ICANN) before March 21, 2001) for use with a certain protocol or application.
Ports with numbers lower than those of the registered ports are called well known ports; ports with numbers greater than those of the registered ports are called dynamic and/or private ports.
Ports 0-1023 - well known ports
Ports 1024-49151 - Registered port: vendors use for applications
Ports >49151 - dynamic / private ports
The other answers are not correct
Reference(s) used for this question:
http://en.wikipedia.org/wiki/Registered_port

NEW QUESTION: 545
Network cabling comes in three flavors, they are:
A. twisted pair, coaxial, and fiber optic.
B. tagged pair, coaxial, and fiber optic.
C. trusted pair, coaxial, and fiber optic.
D. twisted pair, control, and fiber optic.
Answer: A (LEAVE A REPLY)
Network cabling comes in three flavors: twisted pair, coaxial, and fiber optic. Twisted pair
Twisted pair cabling is a form of wiring in which two wires (the forward and return conductors of a single circuit) are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources. This type of cable is used for home and corporate Ethernet networks. Twisted pair cables consist of two insulated copper wires. There are three types of twisted pair cables: Shielded, Unshielded and Foil Fiber Optic cable
An optical fiber cable consists of a center glass core surrounded by several layers of protective material. The outer insulating jacket is made of Teflon or PVC to prevent interference. It is expensive but has higher bandwidth and can transmit data over longer distances. Coaxial cable
Coaxial lines confine the electromagnetic wave to area inside the cable, between the center conductor and the shield. The transmission of energy in the line occurs totally through the dielectric inside the cable between the conductors. Coaxial lines can therefore be bent and twisted (subject to limits) without negative effects, and they can be strapped to conductive supports without inducing unwanted currents in them and though.
The most common use for coaxial cables is for television and other signals with bandwidth of multiple megahertz. Although in most homes coaxial cables have been installed for transmission of TV signals, new technologies (such as the ITU-T G.hn standard) open the possibility of using home coaxial cable for high-speed home networking applications (Ethernet over coax).
See the following page for more details: http://fcit.usf.edu/network/chap4/chap4.htm
Reference used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 101. and Wikipedia at http://en.wikipedia.org/wiki/Networking_cables

NEW QUESTION: 546
When referring to a computer crime investigation, which of the following would be the MOST important step required in order to preserve and maintain a proper chain of custody of evidence:
A. Evidence has to be collected in accordance with all laws and all legal regulations.
B. Law enforcement officials should be contacted for advice on how and when to collect critical information.
C. Verifiable documentation indicating the who, what, when, where, and how the evidence was handled should be available.
D. Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Two concepts that are at the heart of dealing effectively with digital/electronic evidence, or any evidence for that matter, are the chain of custody and authenticity/integrity.
The chain of custody refers to the who, what, when, where, and how the evidence was handled-from its identification through its entire life cycle, which ends with destruction or permanent archiving.
Any break in this chain can cast doubt on the integrity of the evidence and on the professionalism of those directly involved in either the investigation or the collection and handling of the evidence. The chain of custody requires following a formal process that is well documented and forms part of a standard operating procedure that is used in all cases, no exceptions.
The following are incorrect answers:
Evidence has to be collected in accordance with all laws and legal regulations. Evidence would have to be collected in accordance with applicable laws and regulations but not necessarily with ALL laws and regulations.
Only laws and regulations that applies would be followed.
Law enforcement officials should be contacted for advice on how and when to collect critical information. It seems you failed to do your homework, once you have an incident it is a bit late to do this. Proper crime investigation as well as incident response is all about being prepared ahead of time. Obviously, you are improvising if you need to call law enforcement to find out what to do. It is a great way of contaminating your evidence by mistake if you don't have a well documented processs with clear procedures that needs to be followed.
Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation. Specific legal requirements exists for log retention and they are not the same as normal business records. Laws such as Basel, HIPPAA, SOX, and others has specific requirements.
Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 23465-23470). Auerbach Publications. Kindle Edition.
and
ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter
7: Responding to Intrusions (pages 282-285).

NEW QUESTION: 547
The communications products and services, which ensure that the various components of a network (such as devices, protocols, and access methods) work together refers to:
A. Netware Architecture.
B. Network Architecture.
C. WAN Architecture.
D. Multiprotocol Architecture.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
A Network Architecture refers to the communications products and services, which ensure that the various components of a network (such as devices, protocols, and access methods) work together.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 101.

NEW QUESTION: 548
What can best be described as a domain of trust that shares a single security policy and single management?
A. The reference monitor
B. A security domain
C. The security kernel
D. The security perimeter
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
A security domain is a domain of trust that shares a single security policy and single management.
The term security domain just builds upon the definition of domain by adding the fact that resources within this logical structure (domain) are working under the same security policy and managed by the same group.
So, a network administrator may put all of the accounting personnel, computers, and network resources in Domain 1 and all of the management personnel, computers, and network resources in Domain 2.
These items fall into these individual containers because they not only carry out similar types of business functions, but also, and more importantly, have the same type of trust level. It is this common trust level that allows entities to be managed by one single security policy.

The different domains are separated by logical boundaries, such as firewalls with ACLs, directory services making access decisions, and objects that have their own ACLs indicating which individuals and groups can carry out operations on them.
All of these security mechanisms are examples of components that enforce the security policy for each domain. Domains can be architected in a hierarchical manner that dictates the relationship between the different domains and the ways in which subjects within the different domains can communicate. Subjects can access resources in domains of equal or lower trust levels.
The following are incorrect answers:
The reference monitor is an abstract machine which must mediate all access to subjects to objects, be protected from modification, be verifiable as correct, and is always invoked. Concept that defines a set of design requirements of a reference validation mechanism (security kernel), which enforces an access control policy over subjects' (processes, users) ability to perform operations (read, write, execute) on objects (files, resources) on a system. The reference monitor components must be small enough to test properly and be tamperproof.
The security kernel is the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept.
The security perimeter includes the security kernel as well as other security-related system functions that are within the boundary of the trusted computing base. System elements that are outside of the security perimeter need not be trusted. not every process and resource falls within the TCB, so some of these components fall outside of an imaginary boundary referred to as the security perimeter. A security perimeter is a boundary that divides the trusted from the untrusted. For the system to stay in a secure and trusted state, precise communication standards must be developed to ensure that when a component within the TCB needs to communicate with a component outside the TCB, the communication cannot expose the system to unexpected security compromises. This type of communication is handled and controlled through interfaces.
Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 28548-28550). McGraw-Hill. Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 7873-7877). McGraw- Hill. Kindle Edition.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition , Access Control, Page 214-217
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Security Architecture and Design (Kindle Locations 1280-1283). . Kindle Edition.
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
AIO 6th edition chapter 3 access control page 214-217 defines Security domains. Reference monitor, Security Kernel, and Security Parameter are defined in Chapter 4, Security Architecture and Design.

NEW QUESTION: 549
In the context of Biometric authentication, what is a quick way to compare the accuracy of devices. In general, the device that have the lowest value would be the most accurate. Which of the following would be used to compare accuracy of devices?

A. the CER is used.
B. the FRR is used
C. the FAR is used
D. the FER is used
Answer: (SHOW ANSWER)
equal error rate or crossover error rate (EER or CER): the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.
In the context of Biometric Authentication almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher False Reject Rate (FRR).
Conversely, if the sensitivity is decreased, the False Acceptance Rate (FAR) will increase. Thus, to have a valid measure of the system performance, the CrossOver Error Rate (CER) is used.
The following are used as performance metrics for biometric systems:
false accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, then he is treated as genuine that increase the FAR and hence performance also depends upon the selection of threshold value.
false reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
template capacity: the maximum number of sets of data which can be stored in the system.
Reference(s) used for this question: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37. and Wikipedia at: https://en.wikipedia.org/wiki/Biometrics

NEW QUESTION: 550
Which communication method is characterized by very high speed transmission rates that are governed by electronic clock timing signals?
A. Asynchronous Communication.
B. Synchronous Communication.
C. Automatic Communication.
D. Full duplex Communication.
Answer: (SHOW ANSWER)

Synchronous Communication is characterized by very high speed transmission rates that are governed by electronic clock timing signals. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100

NEW QUESTION: 551
Passwords can be required to change monthly, quarterly, or at other intervals:
A. depending on the criticality of the information needing protection
B. depending on the criticality of the information needing protection and the password's frequency of use
C. depending on the password's frequency of use
D. not depending on the criticality of the information needing protection but depending on the password's frequency of use
Answer: (SHOW ANSWER)
Explanation/Reference:
Passwords can be compromised and must be protected. In the ideal case, a password should only be used once. The changing of passwords can also fall between these two extremes. Passwords can be required to change monthly, quarterly, or at other intervals, depending on the criticality of the information needing protection and the password's frequency of use. Obviously, the more times a password is used, the more chance there is of it being compromised.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36 & 37.

NEW QUESTION: 552
Which of the following is an example of a passive attack?
A. Denying services to legitimate users
B. Shoulder surfing
C. Brute-force password cracking
D. Smurfing
Answer: (SHOW ANSWER)
Shoulder surfing is a form of a passive attack involving stealing passwords,
personal identification numbers or other confidential information by looking over someone's
shoulder. All other forms of attack are active attacks, where a threat makes a modification
to the system in an attempt to take advantage of a vulnerability.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-
Hill/Osborne, 2002, chapter 3: Security Management Practices (page 63).

NEW QUESTION: 553
What term describes the amount of risk that remains after the countermeasures have been deployed and the vulnerabilities classified?
A. Residual risk
B. Imminent risk
C. Terminal risk

D. Infinite risk
Answer: A (LEAVE A REPLY)

NEW QUESTION: 554
As per the Orange Book, what are two types of system assurance?
A. Operational Assurance and Architectural Assurance.
B. Design Assurance and Implementation Assurance.
C. Architectural Assurance and Implementation Assurance.
D. Operational Assurance and Life-Cycle Assurance.
Answer: (SHOW ANSWER)
Are the two types of assurance mentioned in the Orange book.
The following answers are incorrect:
Operational Assurance and Architectural Assurance. Is incorrect because Architectural Assurance is not a type of assurance mentioned in the Orange book.
Design Assurance and Implementation Assurance. Is incorrect because neither are types of assurance mentioned in the Orange book.
Architectural Assurance and Implementation Assurance. Is incorrect because neither are types of assurance mentioned in the Orange book.

NEW QUESTION: 555
What can a packet filtering firewall also be called?
A. a scanning router
B. a shielding router
C. a sniffing router
D. a screening router
Answer: (SHOW ANSWER)
While neither CBK nor AIO3 use the term "screening router," they both discuss how the packet filtering capabilities of a router can be used to block traffic much like a packet filtering firewall. Krutz and Vine use this term on p. 90.
"A scanning router" is incorrect. This is a nonsense term to distract you. "A shielding router" is incorrect. This is a nonsense term to distract you. "A sniffing router" is incorrect. This is a nonsense term to distract you.
References:
CBK, p. 433 AIO3, pp.484 - 485

NEW QUESTION: 556
Identification and authentication are the keystones of most access control systems. Identification establishes:
A. User accountability for the actions on the system.
B. Top management accountability for the actions on the system.
C. EDP department accountability for the actions of users on the system.

D. Authentication for actions on the system

Answer: A (LEAVE A REPLY)

Identification and authentication are the keystones of most access control systems. Identification establishes user accountability for the actions on the system.

The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Once a person has been identified through the user ID or a similar value, she must be authenticated, which means she must prove she is who she says she is. Three general factors can be used for authentication: something a person knows, something a person has, and something a person is. They are also commonly called authentication by knowledge, authentication by ownership, and authentication by characteristic.

For a user to be able to access a resource, he first must prove he is who he claims to be, has the necessary credentials, and has been given the necessary rights or privileges to perform the actions he is requesting. Once these steps are completed successfully, the user can access and use network resources; however, it is necessary to track the user's activities and enforce accountability for his actions.

Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. To be properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, passphrase, cryptographic key, personal identification number (PIN), anatomical attribute, or token.

These two credential items are compared to information that has been previously stored for this subject. If these credentials match the stored information, the subject is authenticated. But we are not done yet.

Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions. The system will look at some type of access control matrix or compare security labels to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.

Although identification, authentication, authorization, and accountability have close and complementary definitions, each has distinct functions that fulfill a specific requirement in the process of access control. A user may be properly identified and authenticated to the network, but he may not have the authorization to access the files on the file server. On the other hand, a user may be authorized to access the files on the file server, but until she is properly identified and authenticated, those resources are out of reach.

Reference(s) used for this question:

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Access Control ((ISC)2 Press) (Kindle Locations 889-892). Auerbach Publications. Kindle Edition. and Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3875-3878). McGraw-Hill. Kindle Edition. and Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3833-3848). McGraw-Hill. Kindle Edition. and Source: KRUTZ, Ronald L. & VINES, Russel D.,

The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 557
Which of the following statements do not apply to a hot site?
A. It is expensive.
B. There are cases of common overselling of processing capabilities by the service provider.
C. It provides a false sense of security.
D. It is accessible on a first come first serve basis. In case of large disaster it might not be accessible.
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Remember this is a NOT question. Hot sites do not provide a false sense of security since they are the best disaster recovery alternate for backup site that you rent.
A Cold, Warm, and Hot site is always a rental place in the context of the CBK. This is definivily the best choices out of the rental options that exists. It is fully configured and can be activated in a very short period of time.
Cold and Warm sites, not hot sites, provide a false sense of security because you can never fully test your plan.
In reality, using a cold site will most likely make effective recovery impossible or could lead to business closure if it takes more than two weeks for recovery.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 284).

NEW QUESTION: 558
Which of the following statements pertaining to a Criticality Survey is incorrect?
A. It is implemented to gather input from all personnel that is going to be part of the recovery teams.
B. The purpose of the survey must be clearly stated.
C. Management's approval should be obtained before distributing the survey.
D. Its intent is to find out what services and systems are critical to keeping the organization in business.
Answer: (SHOW ANSWER)

The Criticality Survey is implemented through a standard questionnaire to gather input from the most knowledgeable people. Not all personnel that is going to be part of recovery teams is necessarily able to help in identifying critical functions of the organization.
The intent of such a survey is to identify the services and systems that are critical to the organization. Having a clearly stated purpose for the survey helps in avoiding misinterpretations.
Management's approval of the survey should be obtained before distributing it. Source: HARE, Chris, CISSP Study Guide: Business Continuity Planning Domain,

NEW QUESTION: 559
Which cable technology refers to the CAT3 and CAT5 categories?
A. Coaxial cables
B. Fiber Optic cables
C. Axial cables
D. Twisted Pair cables
Answer: D (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:
Twisted Pair cables currently have two categories in common usage. CAT3 and CAT5.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.

NEW QUESTION: 560
In order to be able to successfully prosecute an intruder:
A. A point of contact should be designated to be responsible for communicating with law enforcement and other external agencies.
B. A proper chain of custody of evidence has to be preserved.
C. Collection of evidence has to be done following predefined procedures.
D. Whenever possible, analyze a replica of the compromised resource, not the original, thereby avoiding inadvertently tamping with evidence.
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
If you intend on prosecuting an intruder, evidence has to be collected in a lawful manner and, most importantly, protected through a secure chain-of-custody procedure that tracks who has been involved in handling the evidence and where it has been stored. All other choices are all important points, but not the best answer, since no prosecution is possible without a proper, provable chain of custody of evidence.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 282-285).

NEW QUESTION: 561
Which of the following is not a component of a Operations Security "triples"?

A. Asset
B. Threat
C. Vulnerability
D. Risk
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation
Explanation/Reference:
The Operations Security domain is concerned with triples - threats, vulnerabilities and assets.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 216.

NEW QUESTION: 562
What is called a password that is the same for each log-on session?
A. "one-time password"
B. "two-time password"
C. static password
D. dynamic password
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION: 563
Which communication method is characterized by very high speed transmission rates that are governed by electronic clock timing signals?
A. Asynchronous Communication.
B. Synchronous Communication.
C. Automatic Communication.
D. Full duplex Communication.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Synchronous Communication is characterized by very high speed transmission rates that are governed by electronic clock timing signals.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 100

NEW QUESTION: 564
Today, privacy violations are almost as serious as security violations?
A. False
B. True

Answer: B (LEAVE A REPLY)

NEW QUESTION: 565
Which of the following is the most complete disaster recovery plan test type, to be performed after successfully completing the Parallel test?
A. Full Interruption test
B. Checklist test
C. Simulation test
D. Structured walk-through test
Answer: A (LEAVE A REPLY)
Explanation/Reference:
The difference between this and the full-interruption test is that the primary production processing of the business does not stop; the test processing runs in parallel to the real processing. This is the most common type of disaster recovery plan testing.
A checklist test is only considered a preliminary step to a real test.
In a structured walk-through test, business unit management representatives meet to walk through the plan, ensuring it accurately reflects the organization's ability to recover successfully, at least on paper.
A simulation test is aimed at testing the ability of the personnel to respond to a simulated disaster, but not recovery process is actually performed.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 289).

NEW QUESTION: 566
Which of the following is NOT a common category/classification of threat to an IT system?
A. Human
B. Natural
C. Technological
D. Hackers
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Hackers are classified as a human threat and not a classification by itself.
All the other answers are incorrect. Threats result from a variety of factors, although they are classified in three types: Natural (e.g., hurricane, tornado, flood and fire), human (e.g. operator error, sabotage, malicious code) or technological (e.g. equipment failure, software error, telecommunications network outage, electric power failure).
Reference:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf, June 2002 (page 6).

NEW QUESTION: 567
Which of the following can be defined as the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors?
A. Unit testing
B. Pilot testing
C. Regression testing
D. Parallel testing
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Regression testing is the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be the same as the data used in the original test. Unit testing refers to the testing of an individual program or module. Pilot testing is a preliminary test that focuses only on specific and predetermined aspects of a system. Parallel testing is the process of feeding test data into two systems and comparing the results.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).

NEW QUESTION: 568
What can be described as a measure of the magnitude of loss or impact on the value of an asset?
A. Probability
B. Exposure factor
C. Vulnerability
D. Threat
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The exposure factor is a measure of the magnitude of loss or impact on the value of an asset.
The probability is the chance or likelihood, in a finite sample, that an event will occur or that a specific loss value may be attained should the event occur.
A vulnerability is the absence or weakness of a risk-reducing safeguard.
A threat is event, the occurrence of which could have an undesired impact.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 3, August 1999.

NEW QUESTION: 569
Which of the following is the most secure form of triple-DES encryption?
A. DES-EDE3
B. DES-EDE1
C. DES-EEE4
D. DES-EDE2

Answer: A (LEAVE A REPLY)
Explanation/Reference:
Triple DES with three distinct keys is the most secure form of triple-DES encryption. It can either be DES-EEE3 (encrypt-encrypt-encrypt) or DES-EDE3 (encrypt-decrypt-encrypt). DES-EDE1 is not defined and would mean using a single key to encrypt, decrypt and encrypt again, equivalent to single DES. DES-EEE4 is not defined and DES-EDE2 uses only 2 keys (encrypt with first key, decrypt with second key, encrypt with first key again).
Source: DUPUIS, Cl?ment, CISSP Open Study Guide on domain 5, cryptography, April 1999.

NEW QUESTION: 570
Which of the following would best classify as a management control?
A. Review of security controls
B. Personnel security
C. Physical and environmental protection
D. Documentation
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Management controls focus on the management of the IT security system and the management of risk for a system.
They are techniques and concerns that are normally addressed by management.
Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system, thus considered management controls.
SECURITY CONTROLS: The management, operational, and technical controls (i.e.,safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
SECURITY CONTROL BASELINE: The set of minimum security controls defined for a low-impact, moderate-impact,or high-impact information system.
The following are incorrect answers:
Personnel security, physical and environmental protection and documentation are forms of operational controls.
Reference(s) used for this question:
http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf and
FIPS PUB 200 at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

NEW QUESTION: 571
The typical computer fraudsters are usually persons with which of the following characteristics?
A. They have had previous contact with law enforcement
B. They conspire with others
C. They hold a position of trust
D. They deviate from the accepted norms of society
Answer: C (LEAVE A REPLY)

Section: Risk, Response and Recovery
Explanation/Reference:
These people, as employees, are trusted to perform their duties honestly and not take advantage of the trust placed in them.
The following answers are incorrect:
They have had previous contact with law enforcement. Is incorrect because most often it is a person that holds a position of trust and this answer implies they have a criminal background. This type of individual is typically not in a position of trust within an organization.
They conspire with others. Is incorrect because they typically work alone, often as a form of retribution over a percieved injustice done to them.
They deviate from the accepted norms of society. Is incorrect because while the nature of fraudsters deviate from the norm, the fraudsters often hold a position of trust within the organization.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 572
Threat assessment has four major components, name them. (Choose four)
A. Type
B. Mechanism
C. Probability
D. Impact
E. ALE - Annual Loss Expectancy
Answer: A,B,C,D (LEAVE A REPLY)

NEW QUESTION: 573
What are the two most critical aspects of risk analysis? (Choose two)
A. Identifying threats
B. Identifying vulnerabilities
C. Identifying resources
D. Identifying assets
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 574
Related to information security, availability is the opposite of which of the following?

A. delegation
B. distribution
C. documentation
D. destruction
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Availability is the opposite of "destruction."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

NEW QUESTION: 575
Which of the following is not one of the three goals of Integrity addressed by the Clark-Wilson model?
A. Prevention of the modification of information by unauthorized users.
B. Prevention of the unauthorized or unintentional modification of information by authorized users.
C. Preservation of the internal and external consistency.
D. Prevention of the modification of information by authorized users.
Answer: A (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
There is no need to prevent modification from authorized users. They are authorized and allowed to make the changes. On top of this, it is also NOT one of the goal of Integrity within Clark-Wilson.
As it turns out, the Biba model addresses only the first of the three integrity goals which is Prevention of the modification of information by unauthorized users. Clark-Wilson addresses all three goals of integrity.
The Clark-Wilson model improves on Biba by focusing on integrity at the transaction level and addressing three major goals of integrity in a commercial environment. In addition to preventing changes by unauthorized subjects, Clark and Wilson realized that high-integrity systems would also have to prevent undesirable changes by authorized subjects and to ensure that the system continued to behave consistently. It also recognized that it would need to ensure that there is constant mediation between every subject and every object if such integrity was going to be maintained.
Integrity is addressed through the following three goals:
1. Prevention of the modification of information by unauthorized users.
2. Prevention of the unauthorized or unintentional modification of information by authorized users.
3. Preservation of the internal and external consistency.
The following reference(s) were used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17689-17694). Auerbach Publications. Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

NEW QUESTION: 576

Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is not a component that achieves this type of security?

A. Administrative control mechanisms

B. Integrity control mechanisms

C. Technical control mechanisms

D. Physical control mechanisms

Answer: B (LEAVE A REPLY)

Integrity Controls Mechanisms are not part of physical security. All of the other detractors were correct this one was the wrong one that does not belong to Physical Security. Below you have more details extracted from the SearchSecurity web site: Information security depends on the security and management of the physical space in which computer systems operate. Domain 9 of the CISSP exam's Common Body of Knowledge addresses the challenges of securing the physical space, its systems and the people who work within it by use of administrative, technical and physical controls. The following questions are covered:

Facilities management: The administrative processes that govern the maintenance and protection of the physical operations space, from site selection through emergency response.

Risks, issues and protection strategies: Risk identification and the selection of security protection components.

Perimeter security: Typical physical protection controls.

Facilities management

Facilities management is a complex component of corporate security that ranges from the planning of a secure physical site to the management of the physical information system environment. Facilities management responsibilities include site selection and physical security planning (i.e. facility construction, design and layout, fire and water damage protection, antitheft mechanisms, intrusion detection and security procedures.) Protections must extend to both people and assets. The necessary level of protection depends on the value of the assets and data. CISSP@ candidates must learn the concept of critical-path analysis as a means of determining a component's business function criticality relative to the cost of operation and replacement. Furthermore, students need to gain an understanding of the optimal location and physical attributes of a secure facility. Among the questions covered in this domain are site inspection, location, accessibility and obscurity, considering the area crime rate, and the likelihood of natural hazards such as floods or earthquakes.

This domain also covers the quality of construction material, such as its protective qualities and load capabilities, as well as how to lay out the structure to minimize risk of forcible entry and accidental damage. Regulatory compliance is also touched on, as is preferred proximity to civil protection services, such as fire and police stations. Attention is given to computer and equipment rooms, including their location, configuration (entrance/egress requirements) and their proximity to wiring distribution centers at the site.

Physical risks, issues and protection strategies

An overview of physical security risks includes risk of theft, service interruption, physical damage, compromised system integrity and unauthorized disclosure of information. Interruptions to business can manifest due to loss of power, services, telecommunications connectivity and water supply. These can also seriously compromise electronic security monitoring alarm/response devices. Backup options are also covered in this domain, as is a strategy for quantifying the risk exposure by simple formula.

Investment in preventive security can be costly. Appropriate redundancy of people skills, systems and infrastructure must be based on the criticality of the data and assets to be preserved. Therefore a strategy is presented that helps determine the selection of cost appropriate controls. Among the questions covered in this domain are regulatory and legal requirements, common standard security protections such as locks and fences, and the importance of establishing service level agreements for maintenance and disaster support. Rounding out the optimization approach are simple calculations for determining mean time between failure and mean time to repair (used to estimate average equipment life expectancy) - essential for estimating the cost/benefit of purchasing and maintaining redundant equipment.

As the lifeblood of computer systems, special attention is placed on adequacy, quality and protection of power supplies. CISSP candidates need to understand power supply concepts and terminology, including those for quality (i.e. transient noise vs. clean power); types of interference (EMI and RFI); and types of interruptions such as power excess by spikes and surges, power loss by fault or blackout, and power degradation from sags and brownouts. A simple formula is presented for determining the total cost per hour for backup power. Proving power reliability through testing is recommended and the advantages of three power protection approaches are discussed (standby UPS, power line conditioners and backup sources) including minimum requirements for primary and alternate power provided.

Environmental controls are explored in this domain, including the value of positive pressure water drains and climate monitoring devices used to control temperature, humidity and reduce static electricity. Optimal temperatures and humidity settings are provided. Recommendations include strict procedures during emergencies, preventing typical risks (such as blocked fans), and the use of antistatic armbands and hygrometers. Positive pressurization for proper ventilation and monitoring for air born contaminants is stressed.

The pros and cons of several detection response systems are deeply explored in this domain. The concept of combustion, the classes of fire and fire extinguisher ratings are detailed. Mechanisms behind smoke-activated, heat-activated and flame-activated devices and Automatic Dial-up alarms are covered, along with their advantages, costs and shortcomings. Types of fire sources are distinguished and the effectiveness of fire suppression methods for each is included. For instance, Halon and its approved replacements are covered, as are the advantages and the inherent risks to equipment of the use of water sprinklers.

Administrative controls The physical security domain also deals with administrative controls applied to physical sites and assets. The need for skilled personnel, knowledge sharing between them, separation of duties, and appropriate oversight in the care and maintenance of equipment and environments is stressed. A list of management duties including hiring checks, employee maintenance activities and

recommended termination procedures is offered. Emergency measures include accountability for evacuation and system shutdown procedures, integration with disaster and business continuity plans, assuring documented procedures are easily available during different types of emergencies, the scheduling of periodic equipment testing, administrative reviews of documentation, procedures and recovery plans, responsibilities delegation, and personnel training and drills.
Perimeter security Domain nine also covers the devices and techniques used to control access to a space. These include access control devices, surveillance monitoring, intrusion detection and corrective actions. Specifications are provided for optimal external boundary protection, including fence heights and placement, and lighting placement and types. Selection of door types and lock characteristics are covered. Surveillance methods and intrusion-detection methods are explained, including the use of video monitoring, guards, dogs, proximity detection systems, photoelectric/photometric systems, wave pattern devices, passive infrared systems, and sound and motion detectors, and current flow sensitivity devices that specifically address computer theft. Room lock types - both preset and cipher locks (and their variations) -- device locks, such as portable laptop locks, lockable server bays, switch control locks and slot locks, port controls, peripheral switch controls and cable trap locks are also covered. Personal access control methods used to identify authorized users for site entry are covered at length, noting social engineering risks such as piggybacking. Wireless proximity devices, both user access and system sensing readers are covered (i.e. transponder based, passive devices and field powered devices) in this domain.
Now that you've been introduced to the key concepts of Domain 9, watch the Domain 9, Physical Security video Return to the CISSP Essentials Security School main page See all SearchSecurity.com's resources on CISSP certification training Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 280.

NEW QUESTION: 577
For which areas of the enterprise are business continuity plans required?
A. All areas of the enterprise.
B. The financial and information processing areas of the enterprise.
C. The operating areas of the enterprise.
D. The marketing, finance, and information processing areas.
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 578
What layer of the ISO/OSI model do routers normally operate at?
A. Data link layer
B. Session layer
C. Transport layer
D. Network layer

Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
Routers are switching devices that operate at the network layer (layer 3) by examining network addresses.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
111).

NEW QUESTION: 579
Which of the following would BEST be defined as an absence or weakness of safeguard that could be exploited?
A. A threat
B. A vulnerability
C. A risk
D. An exposure
Answer: B (LEAVE A REPLY)
It is a software , hardware or procedural weakness that may provide an attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment. A vulnerability characterizes the absence or weakness of a safeguard that could be exploited. This vulnerability may be a service running on a server, unpatched applications or operating system software etc.
The following answers are incorrect because: Threat: A threat is defined as a potential danger to information or systems. The threat is someone or something will identify a specific vulnerability and use it against the company or individual. The entity that takes advantage of a vulnerability is referred to as a 'Threat Agent'. A threat agent could be an intruder accessing the network through a port on the firewall , a process accessing data that violates the security policy. Risk:A risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact. If a firewall has several ports open , there is a higher likelihood that an intruder will use one to access the network in an unauthorized method.
Exposure: An exposure is an instance of being exposed to losses from a threat agent.
REFERENCES: SHON HARRIS , ALL IN ONE THIRD EDITION : Chapter 3 : Security Management Practices , Pages: 57-59

NEW QUESTION: 580
A one way hash converts a string of random length into a _____ encrypted string.
A. fixed length
B. SHA
C. 192 bit
D. 56 bit

E. random length
F. MD5
Answer: A (LEAVE A REPLY)

NEW QUESTION: 581
In discretionary access environments, which of the following entities is authorized to grant information access to other people?
A. Manager
B. Group Leader
C. Security Manager
D. Data Owner
Answer: D (LEAVE A REPLY)
In Discretionary Access Control (DAC) environments, the user who creates a file is also considered the owner and has full control over the file including the ability to set permissions for that file.
The following answers are incorrect:
manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.
group leader. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.
security manager. Is incorrect because in Discretionary Access Control (DAC) environments it is the owner/user that is authorized to grant information access to other people.
IMPORTANT NOTE: The term Data Owner is also used within Classifications as well. Under the subject of classification the Data Owner is a person from management who has been entrusted with a data set that belongs to the company. For example it could be the Chief Financial Officer (CFO) who is entrusted with all of the financial data for a company. As such the CFO would determine the classification of the financial data and who can access as well. The Data Owner would then tell the Data Custodian (a technical person) what the classification and need to know is on the specific set of data.
The term Data Owner under DAC simply means whoever created the file and as the creator of the file the owner has full access and can grant access to other subjects based on their identity.

NEW QUESTION: 582
Macintosh computers are not at risk for receiving viruses.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 583
All of the following can be considered essential business functions that should be identified when creating a Business Impact Analysis (BIA) except one. Which of the following would not be considered an essential element of the BIA but an important TOPIC to include within the BCP plan:
A. IT Network Support

B. Accounting
C. Public Relations
D. Purchasing
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
Public Relations, although important to a company, is not listed as an essential business function that should be identified and have loss criteria developed for.
All other entries are considered essential and should be identified and have loss criteria developed.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9:
Disaster Recovery and Business continuity (page 598).

NEW QUESTION: 584
Which of the following is NOT an advantage that TACACS+ has over TACACS?
A. Event logging
B. Use of two-factor password authentication
C. User has the ability to change his password
D. Ability for security tokens to be resynchronized
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Although TACACS+ provides better audit trails, event logging is a service that is provided with TACACS.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
121).

NEW QUESTION: 585
At which layer of ISO/OSI does the fiber optics work?
A. Network layer
B. Transport layer
C. Data link layer
D. Physical layer
Answer: (SHOW ANSWER)
Section: Network and Telecommunications
Explanation/Reference:
The Answer: Physical layer The Physical layer is responsible for the transmission of the data through the physical medium. This includes such things as cables. Fiber optics is a cabling mechanism which works at Physical layer of OSI model All of the other answers are incorrect.
The following reference(s) were/was used to create this question:
Shon Harris all in one - Chapter 7 (Cabling)

NEW QUESTION: 586
Which of the following would be the best reason for separating the test and development environments?
A. To restrict access to systems under test.
B. To control the stability of the test environment.
C. To segregate user and development staff.
D. To secure access to systems under development.
Answer: B (LEAVE A REPLY)
The test environment must be controlled and stable in order to ensure that development projects are tested in a realistic environment which, as far as possible, mirrors the live environment.
Reference(s) used for this question:
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 309).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 587
Compared to RSA, which of the following is true of Elliptic Curve Cryptography(ECC)?
A. It has been mathematically proved to be more secure.
B. It has been mathematically proved to be less secure.
C. It is believed to require longer key for equivalent security.
D. It is believed to require shorter keys for equivalent security.
Answer: (SHOW ANSWER)
Section: Cryptography
Explanation/Reference:
The following answers are incorrect: It has been mathematically proved to be less secure. ECC has not been proved to be more or less secure than RSA. Since ECC is newer than RSA, it is considered riskier by some, but that is just a general assessment, not based on mathematical arguments.
It has been mathematically proved to be more secure. ECC has not been proved to be more or less secure than RSA. Since ECC is newer than RSA, it is considered riskier by some, but that is just a general assessment, not based on mathematical arguments.

It is believed to require longer key for equivalent security. On the contrary, it is believed to require shorter keys for equivalent security of RSA.
Shon Harris, AIO v5 pg719 states:
"In most cases, the longer the key, the more protection that is provided, but ECC can provide the same level of protection with a key size that is shorter that what RSA requires" The following reference(s) were/was used to create this question:
ISC2 OIG, 2007 p. 258
Shon Harris, AIO v5 pg719

NEW QUESTION: 588
What is the main purpose of Corporate Security Policy?
A. To transfer the responsibility for the information security to all users of the organization
B. To communicate management's intentions in regards to information security
C. To provide detailed steps for performing specific actions
D. To provide a common framework for all development activities
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation
Explanation/Reference:
A Corporate Security Policy is a high level document that indicates what are management`s intentions in regard to Information Security within the organization. It is high level in purpose, it does not give you details about specific products that would be use, specific steps, etc..
The organization's requirements for access control should be defined and documented in its security policies.
Access rules and rights for each user or group of users should be clearly stated in an access policy statement.
The access control policy should minimally consider:
Statements of general security principles and their applicability to the organization Security requirements of individual enterprise applications, systems, and services Consistency between the access control and information classification policies of different systems and networks Contractual obligations or regulatory compliance regarding protection of assets Standards defining user access profiles for organizational roles Details regarding the management of the access control system As a Certified Information System Security Professional (CISSP) you would be involved directly in the drafting and coordination of security policies, standards and supporting guidelines, procedures, and baselines.
Guidance provided by the CISSP for technical security issues, and emerging threats are considered for the adoption of new policies. Activities such as interpretation of government regulations and industry trends and analysis of vendor solutions to include in the security architecture that advances the security of the organization are performed by the CISSP as well.
The following are incorrect answers:

To transfer the responsibility for the information security to all users of the organization is bogus. You CANNOT transfer responsibility, you can only tranfer authority. Responsibility will also sit with upper management. The keyworks ALL and USERS is also an indication that it is the wrong choice.
To provide detailed steps for performing specific actions is also a bogus detractor. A step by step document is referred to as a procedure. It details how to accomplish a specific task.
To provide a common framework for all development activities is also an invalid choice. Security Policies are not restricted only to development activities.
Reference Used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1551-1565). Auerbach Publications. Kindle Edition.
and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 9109-9112). Auerbach Publications. Kindle Edition.

NEW QUESTION: 589
What is the most secure way to dispose of information on a CD-ROM?
A. Sanitizing
B. Physical damage
C. Degaussing
D. Physical destruction
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
First you have to realize that the question is specifically talking about a CDROM. The information stored on a CDROM is not in electro magnetic format, so a degausser woud be inneffective.
You cannot sanitize a CDROM but you might be able to sanitize a RW/CDROM. A CDROM is a write once device and cannot be overwritten like a hard disk or other magnetic device.
Physical Damage would not be enough as information could still be extracted in a lab from the undamaged portion of the media or even from the pieces after the physical damage has been done.
Physical Destruction using a shredder, your microwave oven, melting it, would be very effective and the best choice for a non magnetic media such as a CDROM.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 590
What is the main difference between a Smurf and a Fraggle attack?
A. A Smurf attack is ICMP-based and a Fraggle attack is UDP-based.
B. A Smurf attack is UDP-based and a Fraggle attack is TCP-based.
C. Smurf attack packets cannot be spoofed.
D. A Smurf attack is UDP-based and a Fraggle attack is ICMP-based.
Answer: (SHOW ANSWER)
Section: Network and Telecommunications

Explanation/Reference:
Fraggle is an attack similar to Smurf, but instead of using ICMP, it uses UDP.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11:
Application and System Development (page 790).

NEW QUESTION: 591
Which of the following identifies the encryption algorithm selected by NIST for the new Advanced Encryption Standard?
A. Twofish
B. Serpent
C. RC6
D. Rijndael
Answer: D (LEAVE A REPLY)
Rijndael. Rijndael is the new approved method of encrypting sensitive but unclassified information for the U.S. government. It has been accepted by and is also widely used in the public arena as well. It has low memory requirements and has been constructed to easily defend against timing attacks.
The following answers are incorrect: Twofish. Twofish was among the final candidates chosen for AES, but was not selected.
Serpent. Serpent was among the final candidates chosen for AES, but was not selected. RC6. RC6 was among the final candidates chosen for AES, but was not selected.
The following reference(s) were/was used to create this question:
ISC2 OIG, 2007 p. 622, 629-630 Shon Harris AIO, v.3 p 247-250

NEW QUESTION: 592
Which of the following are Unix / Linux based security tools?
A. Tiger
B. LogCheck
C. All of the tools listed can work on theUnix platforms
D. TripWire
E. TCP Wrappers
F. SATAN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 593
A prolonged complete loss of electric power is a:
A. brownout
B. blackout
C. surge
D. fault
Answer: B (LEAVE A REPLY)

Section: Risk, Response and Recovery
Explanation/Reference:
A prolonged power outage is a blackout.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

NEW QUESTION: 594
Why should batch files and scripts be stored in a protected area?
A. Because of the least privilege concept.
B. Because they cannot be accessed by operators.
C. Because they may contain credentials.
D. Because of the need-to-know concept.
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Because scripts contain credentials, they must be stored in a protected area and the transmission of the scripts must be dealt with carefully. Operators might need access to batch files and scripts. The least privilege concept requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services.
Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

NEW QUESTION: 595
In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?
A. Known-plaintext attack
B. Ciphertext-only attack
C. Chosen-Ciphertext attack
D. Plaintext-only attack
Answer: (SHOW ANSWER)
Explanation/Reference:
In a ciphertext-only attack, the attacker has the ciphertext of several messages encrypted with the same encryption algorithm. Its goal is to discover the plaintext of the messages by figuring out the key used in the encryption process. In a known-plaintext attack, the attacker has the plaintext and the ciphertext of one or more messages. In a chosen-ciphertext attack, the attacker can chose the ciphertext to be decrypted and has access to the resulting plaintext.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter
8: Cryptography (page 578).

NEW QUESTION: 596
Which of the following is the most secure form of triple-DES encryption?
A. DES-EDE3
B. DES-EDE1
C. DES-EEE4
D. DES-EDE2
Answer: (SHOW ANSWER)
Triple DES with three distinct keys is the most secure form of triple-DES encryption. It can either be DES-EEE3 (encrypt-encrypt-encrypt) or DES-EDE3 (encryptdecrypt-encrypt). DES-EDE1 is not defined and would mean using a single key to encrypt, decrypt and encrypt again, equivalent to single DES. DES-EEE4 is not defined and DESEDE2 uses only 2 keys (encrypt with first key, decrypt with second key, encrypt with first key again). Source: DUPUIS, Cl?ment, CISSP Open Study Guide on domain 5, cryptography, April 1999.

NEW QUESTION: 597
Controls are implemented to:
A. eliminate risk and reduce the potential for loss
B. mitigate risk and eliminate the potential for loss
C. mitigate risk and reduce the potential for loss
D. eliminate risk and eliminate the potential for loss
Answer: (SHOW ANSWER)
Explanation/Reference:
Controls are implemented to mitigate risk and reduce the potential for loss. Preventive controls are put in place to inhibit harmful occurrences; detective controls are established to discover harmful occurrences; corrective controls are used to restore systems that are victims of harmful attacks.
It is not feasible and possible to eliminate all risks and the potential for loss as risk/threats are constantly changing.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.

NEW QUESTION: 598
Which of the following statements pertaining to IPSec is incorrect?
A. IPSec can help in protecting networks from some of the IP network attacks.
B. IPSec provides confidentiality and integrity to information transferred over IP networks through transport layer encryption and authentication.
C. IPSec protects against man-in-the-middle attacks.
D. IPSec protects against spoofing.
Answer: (SHOW ANSWER)
Explanation/Reference:

IPSec provides confidentiality and integrity to information transferred over IP networks through network (not transport) layer encryption and authentication. All other statements are correct.
Source: TIPTON, Harold F & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 6, Extranet Access Control Issues (page 110).

NEW QUESTION: 599
What setup should an administrator use for regularly testing the strength of user passwords?
A. A networked workstation so that the live password database can easily be accessed by the cracking program.
B. A networked workstation so the password database can easily be copied locally and processed by the cracking program.
C. A standalone workstation on which the password database is copied and processed by the cracking program.
D. A password-cracking program is unethical; therefore it should not be used.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Poor password selection is frequently a major security problem for any system's security. Administrators should obtain and use password-guessing programs frequently to identify those users having easily guessed passwords.
Because password-cracking programs are very CPU intensive and can slow the system on which it is running, it is a good idea to transfer the encrypted passwords to a standalone (not networked) workstation.
Also, by doing the work on a non-networked machine, any results found will not be accessible by anyone unless they have physical access to that system.
Out of the four choice presented above this is the best choice.
However, in real life you would have strong password policies that enforce complexity requirements and does not let the user choose a simple or short password that can be easily cracked or guessed. That would be the best choice if it was one of the choice presented.
Another issue with password cracking is one of privacy. Many password cracking tools can avoid this by only showing the password was cracked and not showing what the password actually is. It is masking the password being used from the person doing the cracking.
Source: National Security Agency, Systems and Network Attack Center (SNAC), The 60 Minute Network Security Guide, February 2002, page 8.

NEW QUESTION: 600
Of the protocols list, which one is connection oriented?
A. DNS
B. UDP
C. TCP
D. All protocols listed are connection oriented
E. IP

Answer: C (LEAVE A REPLY)

NEW QUESTION: 601
What does "residual risk" mean?
A. The security risk that remains after controls have been implemented
B. Weakness of an assets which can be exploited by a threat
C. Risk that remains after risk assessment has has been performed
D. A security risk intrinsic to an asset being audited, where no mitigation has taken place.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Residual risk is "The security risk that remains after controls have been implemented" ISO/IEC TR 13335-1 Guidelines for the Management of IT Security (GMITS), Part 1: Concepts and Models for IT Security, 1996.
"Weakness of an assets which can be exploited by a threat" is vulnerability. "The result of unwanted incident" is impact. Risk that remains after risk analysis has been performed is a distracter.
Risk can never be eliminated nor avoided, but it can be mitigated, transferred or accpeted. Even after applying a countermeasure like for example putiing up an Antivirus. But still it is not 100% that systems will be protected by antivirus.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 602
Which of the following is the biggest concern with firewall security?
A. Internal hackers
B. Complex configuration rules leading to misconfiguration
C. Buffer overflows
D. Distributed denial of service (DDOS) attacks
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Firewalls tend to give a false sense of security. They can be very hard to bypass but they need to be properly configured. The complexity of configuration rules can introduce a vulnerability when the person responsible for its configuration does not fully understand all possible options and switches. Denial of service attacks mainly concerns availability.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter
3: Telecommunications and Network Security (page 412).

NEW QUESTION: 603
To control access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up:
A. Access Rules
B. Access Matrix
C. Identification controls
D. Access terminal
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Controlling access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up access rules.
These rules can be classified into three access control models: Mandatory, Discretionary, and Non-Discretionary.
An access matrix is one of the means used to implement access control.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION: 604
What is the main characteristic of a bastion host?
A. It is located on the internal network.
B. It is a hardened computer implementation
C. It is a firewall.
D. It does packet filtering.
Answer: (SHOW ANSWER)
A bastion host is a special purpose computer on a network specifically designed and configured to withstand attack. The computer hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer. It is hardened in this manner primarily due to its location and purpose, which is either on the outside of the firewall or in the DMZ and usually involves access from untrusted networks or computers.
References: http://en.wikipedia.org/wiki/Bastion_host

NEW QUESTION: 605
Government categories of data classification include which of the following? (Choose all that apply)
A. Secret
B. Top Secret
C. Confidentiality

D. Availability
E. Need to Know
F. Confidential
Answer: A,B,F (LEAVE A REPLY)

NEW QUESTION: 606
Which of the following is NOT a part of a risk analysis?
A. Identify risks
B. Quantify the impact of potential threats
C. Provide an economic balance between the impact of the risk and the cost of the associated countermeasure
D. Choose the best countermeasure
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
This step is not a part of RISK ANALYSIS.
A risk analysis has three main goals: identify risks, quantify the impact of potential threats, and provide an economic balance between the impact of the risk and the cost of the associated countermeasure.
Choosing the best countermeasure is not part of the risk analysis.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 3:
Security Management Practices (page 73).
HARRIS, Shon, Mike Meyers' CISSP(R) Certification Passport, 2002, McGraw-Hill, page 12.

NEW QUESTION: 607
What is the most secure way to dispose of information on a CD-ROM?
A. Sanitizing
B. Physical damage
C. Degaussing
D. Physical destruction
Answer: D (LEAVE A REPLY)
Explanation/Reference:
First you have to realize that the question is specifically talking about a CDROM. The information stored on a CDROM is not in electro magnetic format, so a degausser woud be inneffective.
You cannot sanitize a CDROM but you might be able to sanitize a RW/CDROM. A CDROM is a write once device and cannot be overwritten like a hard disk or other magnetic device.
Physical Damage would not be enough as information could still be extracted in a lab from the undamaged portion of the media or even from the pieces after the physical damage has been done.
Physical Destruction using a shredder, your microwave oven, melting it, would be very effective and the best choice for a non magnetic media such as a CDROM.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 608
Which of the following results in the most devastating business interruptions?
A. Loss of Hardware/Software
B. Loss of Data
C. Loss of Communication Links
D. Loss of Applications
Answer: (SHOW ANSWER)
Section: Risk, Response and Recovery
Explanation/Reference:
Source: Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1.
All of the others can be replaced or repaired. Data that is lost and was not backed up, cannot be restored.

NEW QUESTION: 609
What refers to legitimate users accessing networked services that would normally be restricted to them?
A. Spoofing
B. Piggybacking
C. Eavesdropping
D. Logon abuse
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Unauthorized access of restricted network services by the circumvention of security access controls is known as logon abuse. This type of abuse refers to users who may be internal to the network but access resources they would not normally be allowed.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
74).

NEW QUESTION: 610
The principle of least privilege is effective in helping prevent security breaches, however, prevention works best when applied with _____ and _____. Together, these three complete a security triad. (Choose two)
A. Footprinting
B. Scanning
C. Attack
D. Detection
E. Response
Answer: D,E (LEAVE A REPLY)
Prevention, detection, and response form the basis of an effective security stance. Least privilege helps provides prevention. Detection is needed because program bugs or human errors have the potential to

cause security breaches. Security policy must be monitored for violations to determine an adequate response.

NEW QUESTION: 611
Which one of the following factors is NOT one on which Authentication is based?
A. Type 1. Something you know, such as a PIN or password
B. Type 2. Something you have, such as an ATM card or smart card
C. Type 3. Something you are (based upon one or more intrinsic physical or behavioral traits), such as a fingerprint or retina scan
D. Type 4. Something you are, such as a system administrator or security administrator
Answer: D (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Authentication is based on the following three factor types:
Type 1. Something you know, such as a PIN or password
Type 2. Something you have, such as an ATM card or smart card
Type 3. Something you are (Unique physical characteristic), such as a fingerprint or retina scan Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.
Also: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4:
Access Control (pages 132-133).

NEW QUESTION: 612
It is a violation of the "separation of duties" principle when which of the following individuals access the software on systems implementing security?
A. security administrator
B. security analyst
C. systems auditor
D. systems programmer
Answer: D (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation
Explanation/Reference:
Reason: The security administrator, security analysis, and the system auditor need access to portions of the security systems to accomplish their jobs. The system programmer does not need access to the working (AKA: Production) security systems.
Programmers should not be allowed to have ongoing direct access to computers running production systems (systems used by the organization to operate its business). To maintain system integrity, any changes they make to production systems should be tracked by the organization's change management control system.

Because the security administrator's job is to perform security functions, the performance of non-security tasks must be strictly limited. This separation of duties reduces the likelihood of loss that results from users abusing their authority by taking actions outside of their assigned functional responsibilities.
References:
OFFICIAL (ISC)2 GUIDE TO THE CISSP EXAM (2003), Hansche, S., Berti, J., Hare, H., Auerbach Publication, FL, Chapter 5 - Operations Security, section 5.3,"Security Technology and Tools," Personnel section (page 32).
KRUTZ, R. & VINES, R. The CISSP Prep Guide: Gold Edition (2003), Wiley Publishing Inc., Chapter 6: Operations Security, Separations of Duties (page 303).

NEW QUESTION: 613
Which of the following is most concerned with personnel security?
A. Management controls
B. Operational controls
C. Technical controls
D. Human resources controls
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Many important issues in computer security involve human users, designers, implementers, and managers.
A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. Since operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems), personnel security is considered a form of operational control.
Operational controls are put in place to improve security of a particular system (or group of systems). They often require specialized expertise and often rely upon management activities as well as technical controls.
Implementing dual control and making sure that you have more than one person that can perform a task would fall into this category as well.
Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.
Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access of misuse, facilitate detection of security violations, and support security requirements for applications and data.
Reference use for this question:
NIST SP 800-53 Revision 4 http://dx.doi.org/10.6028/NIST.SP.800-53r4
You can get it as a word document by clicking HERE
NIST SP 800-53 Revision 4 has superseded the document below:
SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Page A-18).

NEW QUESTION: 614
Which security model introduces access to objects only through programs?
A. The Biba model
B. The Bell-LaPadula model
C. The Clark-Wilson model
D. The information flow model
Answer: C (LEAVE A REPLY)
In the Clark-Wilson model, the subject no longer has direct access to objects
but instead must access them through programs (well -formed transactions).
The Clark-Wilson integrity model provides a foundation for specifying and analyzing an integrity policy for a computing system.
The model is primarily concerned with formalizing the notion of information integrity.
Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules.
Clark-Wilson is more clearly applicable to business and industry processes in which the integrity of the information content is paramount at any level of classification.
Integrity goals of Clark-Wilson model:
Prevent unauthorized users from making modification (Only this one is addressed by the Biba model).
Separation of duties prevents authorized users from making improper modifications.
Well formed transactions: maintain internal and external consistency i.e. it is a series of operations that are carried out to transfer the data from one consistent state to the other.
The following are incorrect answers:
The Biba model is incorrect. The Biba model is concerned with integrity and controls access to objects based on a comparison of the security level of the subject to that of the object.
The Bell-LaPdaula model is incorrect. The Bell-LaPaula model is concerned with confidentiality and controls access to objects based on a comparison of the clearence level of the subject to the classification level of the object.
The information flow model is incorrect. The information flow model uses a lattice where objects are labelled with security classes and information can flow either upward or at the same level. It is similar in framework to the Bell-LaPadula model.
References:
ISC2 Official Study Guide, Pages 325 - 327 AIO3, pp. 284 - 287 AIOv4 Security Architecture and Design (pages 338 - 342) AIOv5 Security Architecture and Design (pages 341 - 344) Wikipedia at: https://en.wikipedia.org/wiki/Clark-Wilson_model

NEW QUESTION: 615

Information security policies are a _____.
A. Business enabler
B. All of the answers are correct
C. Inconvenience for the end user
D. Necessary evil
E. Waste of time
Answer: (SHOW ANSWER)

NEW QUESTION: 616
What assesses potential loss that could be caused by a disaster?
A. The Business Assessment (BA)
B. The Business Impact Analysis (BIA)
C. The Risk Assessment (RA)
D. The Business Continuity Plan (BCP)
Answer: B (LEAVE A REPLY)
Explanation/Reference:
The Business Assessment is divided into two components. Risk Assessment (RA) and Business Impact Analysis (BIA). Risk Assessment is designed to evaluate existing exposures from the organization's environment, whereas the BIA assesses potential loss that could be caused by a disaster. The Business Continuity Plan's goal is to reduce the risk of financial loss by improving the ability to recover and restore operations efficiently and effectively.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 57).
And: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 276).

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 617
Identification and authentication are the keystones of most access control systems. Identification establishes:
A. User accountability for the actions on the system.
B. Top management accountability for the actions on the system.

C. EDP department accountability for the actions of users on the system.
D. Authentication for actions on the system
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Identification and authentication are the keystones of most access control systems. Identification establishes user accountability for the actions on the system.
The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.
Once a person has been identified through the user ID or a similar value, she must be authenticated, which means she must prove she is who she says she is. Three general factors can be used for authentication:
something a person knows, something a person has, and something a person is. They are also commonly called authentication by knowledge, authentication by ownership, and authentication by characteristic.
For a user to be able to access a resource, he first must prove he is who he claims to be, has the necessary credentials, and has been given the necessary rights or privileges to perform the actions he is requesting.
Once these steps are completed successfully, the user can access and use network resources; however, it is necessary to track the user's activities and enforce accountability for his actions.
Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. To be properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, passphrase, cryptographic key, personal identification number (PIN), anatomical attribute, or token.
These two credential items are compared to information that has been previously stored for this subject. If these credentials match the stored information, the subject is authenticated. But we are not done yet.
Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions. The system will look at some type of access control matrix or compare security labels to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.
Although identification, authentication, authorization, and accountability have close and complementary definitions, each has distinct functions that fulfill a specific requirement in the process of access control. A user may be properly identified and authenticated to the network, but he may not have the authorization to access the files on the file server. On the other hand, a user may be authorized to access the files on the file server, but until she is properly identified and authenticated, those resources are out of reach.
Reference(s) used for this question:

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Access Control ((ISC)
2 Press) (Kindle Locations 889-892). Auerbach Publications. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3875-3878). McGraw- Hill. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3833-3848). McGraw- Hill. Kindle Edition.
and
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION: 618
The IP header contains a protocol field. If this field contains the value of 6, what type of data is contained within the ip datagram?
A. TCP.
B. ICMP.
C. UDP.
D. IGMP.
Answer: A (LEAVE A REPLY)
If the protocol field has a value of 6 then it would indicate it was TCP. The protocol field of the IP packet dictates what protocol the IP packet is using.
TCP=6, ICMP=1, UDP=17, IGMP=2
The following answers are incorrect:
ICMP. Is incorrect because the value for an ICMP protocol would be 1.
UDP. Is incorrect because the value for an UDP protocol would be 17.
IGMP. Is incorrect because the value for an IGMP protocol would be 2.
References:
SANS http://www.sans.org/resources/tcpip.pdf?ref=3871

NEW QUESTION: 619
What is one disadvantage of content-dependent protection of information?
A. It increases processing overhead.
B. It requires additional password entry.
C. It exposes the system to data locking.
D. It limits the user's individual address space.
Answer: A (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION: 620
What prevents a process from accessing another process' data?
A. Memory segmentation
B. Process isolation
C. The reference monitor
D. Data hiding
Answer: B (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Process isolation is where each process has its own distinct address space for its application code and data. In this way, it is possible to prevent each process from accessing another process' data. This prevents data leakage, or modification to the data while it is in memory. Memory segmentation is a virtual memory management mechanism. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. Data hiding, also known as information hiding, is a mechanism that makes information available at one processing level is not available at another level.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION: 621
Which of the following is the most secure firewall implementation?
A. Dual-homed host firewalls
B. Screened-subnet firewalls
C. Screened-host firewalls
D. Packet-filtering firewalls
Answer: B (LEAVE A REPLY)
Explanation/Reference:
One the most secure implementations of firewall architectures is the screened-subnet firewall. It employs two packet-filtering routers and a bastion host. Like a screened host firewall, this firewall supports both packet-filtering and proxy services.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page
93).

NEW QUESTION: 622
Which of the following statements pertaining to a security policy is incorrect?
A. Its main purpose is to inform the users, administrators and managers of their obligatory requirements for protecting technology and information assets.
B. It specifies how hardware and software should be used throughout the organization.

C. It needs to have the acceptance and support of all levels of employees within the organization in order for it to be appropriate and effective.
D. It must be flexible to the changing environment.
Answer: (SHOW ANSWER)
Section: Security Operation Adimnistration
Explanation/Reference:
A security policy would NOT define how hardware and software should be used throughout the organization. A standard or a procedure would provide such details but not a policy.
A security policy is a formal statement of the rules that people who are given access to anorganization's technology and information assets must abide. The policy communicates the security goals to all of the users, the administrators, and the managers. The goals will be largely determined by the following key tradeoffs:
services offered versus security provided, ease of use versus security, and cost of security versus risk of loss.
The main purpose of a security policy is to inform the users, the administrators and the managers of their obligatory requirements for protecting technology and information assets.
The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. A good security policy must:
* Be able to be implemented through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods
* Be able to be enforced with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible
* Clearly define the areas of responsibility for the users, the administrators, and the managers
* Be communicated to all once it is established
* Be flexible to the changing environment of a computer network since it is a living document
Reference(s) used for this question:
National Security Agency, Systems and Network Attack Center (SNAC),The 60 Minute Network Security Guide, February 2002, page 7.
or
A local copy is kept at:
https://www.freepracticetests.org/documents/The%2060%20Minute%20Network%20Security%20Guide.pdf

NEW QUESTION: 623
Once evidence is seized, a law enforcement officer should emphasize which of the following?
A. Chain of command
B. Chain of custody
C. Chain of control

D. Chain of communications
Answer: B (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
All people that handle the evidence from the time the crime was committed through the final disposition must be identified. This is to ensure that the evidence can be used and has not been tampered with.
The following answers are incorrect:
chain of command. Is incorrect because chain of command is the order of authority and does not apply to evidence.
chain of control. Is incorrect because it is a distractor.
chain of communications. Is incorrect because it is a distractor.

NEW QUESTION: 624
Failure of a contingency plan is usually:
A. A technical failure.
B. A management failure.
C. Because of a lack of awareness.
D. Because of a lack of training.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Failure of a contingency plan is usually management failure to exhibit ongoing interest and concern about the BCP/DRP effort, and to provide financial and other resources as needed. Lack of management support will result in a lack awareness and training.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 9: Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) (page 163).

NEW QUESTION: 625
Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?
A. Steganography
B. Digital watermarking
C. Digital enveloping
D. Digital signature
Answer: B (LEAVE A REPLY)
Section: Cryptography
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines digital watermarking as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data-text, graphics, images, video, or audio#and for detecting or extracting the marks later. The set of embedded bits (the digital watermark) is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. It is used as a measure to protect intellectual property rights. Steganography involves hiding the very existence of a message. A

digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. A digital envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 626
Within the realm of IT security, which of the following combinations best defines risk?
A. Threat coupled with a breach
B. Threat coupled with a vulnerability
C. Vulnerability coupled with an attack
D. Threat coupled with a breach of security
Answer: (SHOW ANSWER)
Explanation/Reference:
Threat coupled with a vulnerability. Threats are circumstances or actions with the ability to harm a system. They can destroy or modify data or result an a DoS. Threats by themselves are not acted upon unless there is a vulnerability that can be taken advantage of. Risk enters the equation when a vulnerability (Flaw or weakness) exists in policies, procedures, personnel management, hardware, software or facilities and can be exploited by a threat agent. Vulnerabilities do not cause harm, but they leave the system open to harm. The combination of a threat with a vulnerability increases the risk to the system of an intrusion.
The following answers are incorrect:
Threat coupled with a breach. A threat is the potential that a particular threat-source will take advantage of a vulnerability. Breaches get around security. It does not matter if a breach is discovered or not, it has still occured and is not a risk of something occuring. A breach would quite often be termed as an incident or intrusion.
Vulnerability coupled with an attack. Vulnerabilities are weaknesses (flaws) in policies, procedures, personnel management, hardware, software or factilities that may result in a harmful intrusion to an IT system. An attack takes advantage of the flaw or vulnerability. Attacks are explicit attempts to violate security, and are more than risk as they are active.
Threat coupled with a breach of security. This is a detractor. Although a threat agent may take advantage of (Breach) vulnerabilities or flaws in systems security. A threat coupled with a breach of security is more than a risk as this is active.
The following reference(s) may be used to research the Qs in this question:
ISC2 OIG, 2007 p. 66-67
Shon Harris AIO v3 p. 71-72

NEW QUESTION: 627
Public Key Infrastructure (PKI) uses asymmetric key encryption between parties. The originator encrypts information using the intended recipient's "public" key in order to get confidentiality of the data being sent.

The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology ensures that:

A. The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.

B. The channels through which the information flows are secure.

C. The recipient's identity can be positively verified by the sender.

D. The sender of the message is the only other person with access to the recipient's private key.

Answer: (SHOW ANSWER)

Explanation/Reference:

Through the use of Public Key Infrastructure (PKI) the recipient's identity can be positively verified by the sender.

The sender of the message knows he is using a Public Key that belongs to a specific user. He can validate through the Certification Authority (CA) that a public key is in fact the valid public key of the receiver and the receiver is really who he claims to be. By using the public key of the recipient, only the recipient using the matching private key will be able to decrypt the message. When you wish to achieve confidentiality, you encrypt the message with the recipient public key.

If the sender would wish to prove to the recipient that he is really who he claims to be then the sender would apply a digital signature on the message before encrypting it with the public key of the receiver. This would provide Confidentiality and Authenticity of the message.

A PKI (Public Key Infrastructure) enables users of an insecure public network, such as the Internet, to securely and privately exchange data through the use of public key-pairs that are obtained and shared through a trusted authority, usually referred to as a Certificate Authority.

The PKI provides for digital certificates that can vouch for the identity of individuals or organizations, and for directory services that can store, and when necessary, revoke those digital certificates. A PKI is the underlying technology that addresses the issue of trust in a normally untrusted environment.

The following answers are incorrect:

The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use. Is incorrect because through the use of Public Key Infrastructure (PKI), the parties do not have to have a mutual agreement. They have a trusted 3rd party Certificate Authority to perform the verification of the sender.

The channels through which the information flows are secure. Is incorrect because the use of Public Key Infrastructure (PKI) does nothing to secure the channels.

The sender of the message is the only other person with access to the recipient's private key. Is incorrect because the sender does not have access to the recipient's private key though Public Key Infrastructure (PKI).

Reference(s) used for this question:

OIG CBK Cryptography (pages 253 - 254)

NEW QUESTION: 628

One of the following assertions is NOT a characteristic of Internet Protocol Security (IPsec)

A. Data cannot be read by unauthorized parties

B. The identity of all IPsec endpoints are confirmed by other endpoints
C. Data is delivered in the exact order in which it is sent
D. The number of packets being exchanged can be counted.
Answer: (SHOW ANSWER)
IPSec provide replay protection that ensures data is not delivered multiple times, however IPsec does not ensure that data is delivered in the exact order in which it is sent. IPSEC uses TCP and packets may be delivered out of order to the receiving side depending which route was taken by the packet.
Internet Protocol Security (IPsec) has emerged as the most commonly used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over IP networks. Depending on how IPsec is implemented and configured, it can provide any combination of the following types of protection:
Confidentiality. IPsec can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.
Integrity. IPsec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.
Peer Authentication. Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.
Replay Protection. The same data is not delivered multiple times, and data is not delivered grossly out of order. However, IPsec does not ensure that data is delivered in the exact order in which it is sent.
Traffic Analysis Protection. A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged. However, the number of packets being exchanged can be counted.
Access Control. IPsec endpoints can perform filtering to ensure that only authorized IPsec users can access particular network resources. IPsec endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing.
The following are incorrect answers because they are all features provided by IPSEC:
"Data cannot be read by unauthorized parties" is wrong because IPsec provides confidentiality through the usage of the Encapsulating Security Protocol (ESP), once encrypted the data cannot be read by unauthorized parties because they have access only to the ciphertext. This is accomplished by encrypting data using a cryptographic algorithm and a session key, a value known only to the two parties exchanging data. The data can only be decrypted by someone who has a copy of the session key.
"The identity of all IPsec endpoints are confirmed by other endpoints" is wrong because IPsec provides peer authentication: Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.
"The number of packets being exchanged can be counted" is wrong because although IPsec provides traffic protection where a person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged, the number of packets being exchanged still can be counted.

Reference(s) used for this question:
NIST 800-77 Guide to IPsec VPNs . Pages 2-3 to 2-4

NEW QUESTION: 629
A weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks is called a ?
A. Vulnerability
B. Risk
C. Threat
D. Overflow
Answer: A (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
The Answer: Vulnerability; Vulnerability is a weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

NEW QUESTION: 630
The general philosophy for DMZ's is that:
A. any system on the DMZ can be compromized because it's accessible from the Internet.
B. any system on the DMZ cannot be compromized because it's not accessible from the Internet.
C. some systems on the DMZ can be compromized because they are accessible from the Internet.
D. any system on the DMZ cannot be compromized because it's by definition 100 percent safe and not accessible from the Internet.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Because the DMZ systems are accessible from the Internet, they are more at risk for attacka nd compromise and must be hardened appropriately.
"Any system on the DMZ cannot be compromised because it's not accessible from the Internet" is incorrect. The reason a system is placed in the DMZ is so it can be accessible from the Internet.
"Some systems on the DMZ can be compromised because they are accessible from the Internet" is incorrect. All systems in the DMZ face an increased risk of attack and compromise because they are accessible from the Internet.
"Any system on the DMZ cannot be compromised because it's by definition 100 percent safe and not accessible from the Internet" is incorrect. Again, a system is placed in the DMZ because it must be accessible from the Internet.
References:
CBK, p. 434
AIO3, p. 483

NEW QUESTION: 631
A packet containing a long string of NOP's followed by a command is usually indicative of what?
A. A syn scan.
B. A half-port scan.
C. A buffer overflow attack.
D. A packet destined for the network's broadcast address.
Answer: (SHOW ANSWER)
A series of the same control, hexidecimal, characters imbedded in the string is usually an indicator of a buffer overflow attack. A NOP is a instruction which does nothing (No Operation - the hexadecimal equivalent is 0x90)
The following answers are incorrect:
A syn scan. This is incorrect because a SYN scan is when a SYN packet is sent to a specific port and the results are then analyzed.
A half-port scan. This is incorrect because the port scanner generates a SYN packet. If the target port is open, it will respond with a SYN-ACK packet. The scanner host responds with a RST packet, closing the connection before the handshake is completed. Also known as a Half Open Port scan.
A packet destined for the network's broadcast address. This is incorrect because this type of packet would not contain a long string of NOP characters.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 632
Which of the following are valid modes of operation? (Choose all that apply)
A. Multilevel mode
B. Restricted mode
C. Dedicated mode
D. Allowed mode
E. Access Mode
Answer: A,C (LEAVE A REPLY)
The four modes of operation include: dedicated mode, system-high mode, compartmented mode, and multilevel mode.

NEW QUESTION: 633
Which of the following encryption algorithms does not deal with discrete logarithms?

A. El Gamal
B. Diffie-Hellman
C. RSA
D. Elliptic Curve
Answer: C (LEAVE A REPLY)
The security of the RSA system is based on the assumption that factoring the product into two original large prime numbers is difficult
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 159). Shon Harris, CISSP All-in-One Examine Guide, Third Edition, McGraw-Hill Companies, August 2005, Chapter 8: Cryptography, Page 636 - 639

NEW QUESTION: 634
Organizations should consider which of the following first before allowing external access to their LANs via the Internet?
A. plan for implementing workstation locking mechanisms.
B. plan for protecting the modem pool.
C. plan for providing the user with his account usage information.
D. plan for considering proper authentication options.
Answer: (SHOW ANSWER)
Explanation/Reference:
Before a LAN is connected to the Internet, you need to determine what the access controls mechanisms are to be used, this would include how you are going to authenticate individuals that may access your network externally through access control.
The following answers are incorrect:
plan for implementing workstation locking mechanisms. This is incorrect because locking the workstations have no impact on the LAN or Internet access.
plan for protecting the modem pool. This is incorrect because protecting the modem pool has no impact on the LAN or Internet access, it just protects the modem.
plan for providing the user with his account usage information. This is incorrect because the question asks what should be done first. While important your primary concern should be focused on security.

NEW QUESTION: 635
Which of the following is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length?
A. Fiber Optic cable
B. Coaxial cable
C. Twisted Pair cable
D. Axial cable
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications

Explanation/Reference:
Fiber Optic cable is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length (up to two kilometers in some cases).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.

NEW QUESTION: 636
Which of the following protocols is designed to send individual messages securely?
A. Kerberos
B. Secure Electronic Transaction (SET).
C. Secure Sockets Layer (SSL).
D. Secure HTTP (S-HTTP).
Answer: D (LEAVE A REPLY)
Explanation/Reference:
An early standard for encrypting HTTP documents, Secure HTTP (S-HTTP) is designed to send individual messages securely. SSL is designed to establish a secure connection between two computers. SET was originated by VISA and MasterCard as an Internet credit card protocol using digital signatures. Kerberos is an authentication system.
Source: KRUTZ, Ronald L & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 89.

NEW QUESTION: 637
Which of the following is a token-passing scheme like token ring that also has a second ring that remains dormant until an error condition is detected on the primary ring?
A. Fiber Distributed Data Interface (FDDI).
B. Ethernet
C. Fast Ethernet
D. Broadband
Answer: A (LEAVE A REPLY)
Explanation/Reference:
FDDI is a token-passing ring scheme like a token ring, yet it also has a second ring that remains dormant until an error condition is detected on the primary ring.
Fiber Distributed Data Interface (FDDI) provides a 100 Mbit/s optical standard for data transmission in a local area network that can extend in range up to 200 kilometers (124 miles). Although FDDI logical topology is a ring-based token network, it does not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol is derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium it uses optical fiber, although it can use copper cable, in which case it may be refer to as CDDI (Copper Distributed Data Interface). FDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology.

Ethernet is a family of frame-based computer networking technologies for local area networks (LANs). The name came from the physical concept of the ether. It defines a number of wiring and signaling standards for the Physical Layer of the OSI networking model as well as a common addressing format and Media Access Control at the Data Link Layer.
In computer networking, Fast Ethernet is a collective term for a number of Ethernet standards that carry traffic at the nominal rate of 100 Mbit/s, against the original Ethernet speed of 10 Mbit/s. Of the fast Ethernet standards 100BASE-TX is by far the most common and is supported by the vast majority of Ethernet hardware currently produced. Fast Ethernet was introduced in 1995 and remained the fastest version of Ethernet for three years before being superseded by gigabit Ethernet.
Broadband in data can refer to broadband networks or broadband Internet and may have the same meaning as above, so that data transmission over a fiber optic cable would be referred to as broadband as compared to a telephone modem operating at 56,000 bits per second. However, a worldwide standard for what level of bandwidth and network speeds actually constitute Broadband have not been determined. [1] Broadband in data communications is frequently used in a more technical sense to refer to data transmission where multiple pieces of data are sent simultaneously to increase the effective rate of transmission, regardless of data signaling rate. In network engineering this term is used for methods where two or more signals share a medium.[Broadband Internet access, often shortened to just broadband, is a high data rate Internet access-typically contrasted with dial-up access using a 56k modem.
Dial-up modems are limited to a bitrate of less than 56 kbit/s (kilobits per second) and require the full use of a telephone line-whereas broadband technologies supply more than double this rate and generally without disrupting telephone use.
Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.
also see:
http://en.wikipedia.org/

NEW QUESTION: 638
Which of the following does NOT concern itself with key management?
A. Internet Security Association Key Management Protocol (ISAKMP)
B. Diffie-Hellman (DH)
C. Cryptology (CRYPTO)
D. Key Exchange Algorithm (KEA)
Answer: C (LEAVE A REPLY)
Cryptology is the science that includes both cryptography and cryptanalysis and is not directly concerned with key management. Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis.
The following are all concerned with Key Management which makes them the wrong choices: Internet Security Association Key Management Protocol (ISAKMP) is a key management protocol used by IPSec. ISAKMP (Internet Security Association and Key Management Protocol) is a protocol defined by RFC

2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange. The actual key exchange is done by the Oakley Key Determination Protocol which is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie-Hellman key exchange algorithm.
Diffie-Hellman and one variation of the Diffie-Hellman algorithm called the Key Exchange Algorithm (KEA) are also key exchange protocols. Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. Diffie-Hellman key exchange (D-H) is a specific method of exchanging keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
Reference(s) used for this question:
Mike Meyers CISSP Certification Passport, by Shon Harris and Mike Meyers, page 228. It is highlighted as an EXAM TIP. Which tells you that it is a must know for the purpose of the exam. HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Chapter 8: Cryptography (page 713-715). and https://en.wikipedia.org/wiki/ISAKMP and
http://searchsecurity.techtarget.com/definition/cryptology

NEW QUESTION: 639
The primary service provided by Kerberos is which of the following?
A. non-repudiation
B. confidentiality
C. authentication
D. authorization
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The Answer: authentication. Kerberos is an authentication service. It can use single-factor or multi-factor authentication methods.
The following answers are incorrect:
non-repudiation. Since Kerberos deals primarily with symmetric cryptography, it does not help with non-repudiation.
confidentiality. Once the client is authenticated by Kerberos and obtains its session key and ticket, it may use them to assure confidentiality of its communication with a server; however, that is not a Kerberos service as such.
authorization. Although Kerberos tickets may include some authorization information, the meaning of the authorization fields is not standardized in the Kerberos specifications, and authorization is not a primary Kerberos service.
The following reference(s) were/was used to create this question:

ISC2 OIG,2007 p. 179-184
Shon Harris AIO v.3 152-155

NEW QUESTION: 640
Which of the following steps is NOT one of the eight detailed steps of a Business Impact Assessment (BIA):
A. Notifying senior management of the start of the assessment.
B. Creating data gathering techniques.
C. Identifying critical business functions.
D. Calculating the risk for each different business function.
Answer: A (LEAVE A REPLY)
Source: HARRIS, S., CISSP All- In-One Exam Guide, 3rd. Edition, 2005, Chapter 9, Page 701.
There have been much discussion about the steps of the BIA and I struggled with this before deciding to scrape the question about "the four steps," and re-write the question using the AIO for a reference. This question should be easy.... if you know all eight steps.
The eight detailed and granular steps of the BIA are:
1.Select Individuals to interview for the data gathering.
2.Create data gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3.Identify the company's critical business functions.
4.Identify the resources that these functions depend upon.
5.Calculate how long these functions can survive without these resources.
6.Identify vulnerabilities and the threats to these functions.
7.Calculate risk for each of the different business functions.
8.Document findings and report them to management.
Shon goes on to cover each step in Chapter 9.

NEW QUESTION: 641
Which of the following focuses on sustaining an organization's business functions during and after a disruption?
A. Business continuity plan
B. Business recovery plan
C. Continuity of operations plan
D. Disaster recovery plan
Answer: A (LEAVE A REPLY)
A business continuity plan (BCP) focuses on sustaining an organization's business functions during and after a disruption. Information systems are considered in the BCP only in terms of their support to the larger business processes. The business recovery plan (BRP) addresses the restoration of business processes after an emergency. The BRP is similar to the BCP, but it typically lacks procedures to ensure continuity of critical processes throughout an emergency or disruption. The continuity of operations plan (COOP) focuses on restoring an organization's essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. The disaster recovery plan (DRP)

applies to major, usually catastrophic events that deny access to the normal facility for an extended period. A DRP is narrower in scope than an IT contingency plan in that it does not address minor disruptions that do not require relocation.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 8).

NEW QUESTION: 642
Which security model is based on the military classification of data and people with clearances?
A. Brewer-Nash model
B. Clark-Wilson model
C. Bell-LaPadula model
D. Biba model
Answer: C (LEAVE A REPLY)
Section: Access Control
Explanation/Reference:
The Bell-LaPadula model is a confidentiality model for information security based on the military classification of data, on people with clearances and data with a classification or sensitivity model. The Biba, Clark-Wilson and Brewer-Nash models are concerned with integrity.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NEW QUESTION: 643
Corporate networks are safer if an end user connects through a VPN connection?
A. False
B. True
Answer: A (LEAVE A REPLY)

NEW QUESTION: 644
You have been tasked to develop an effective information classification program. Which one of the following steps should be performed first?
A. Establish procedures for periodically reviewing the classification and ownership
B. Specify the security controls required for each classification level
C. Identify the data custodian who will be responsible for maintaining the security level of data
D. Specify the criteria that will determine how data is classified
Answer: D (LEAVE A REPLY)
According to the AIO 3rd edition, these are the necessary steps for a proper classification program:
1.Define classification levels.
2.Specify the criteria that will determine how data is classified.
3.Have the data owner indicate the classification of the data she is responsible for.
4.Identify the data custodian who will be responsible for maintaining data and its security level.

5.Indicate the security controls, or protection mechanisms, that are required for each classification level.
6.Document any exceptions to the previous classification issues.
7.Indicate the methods that can be used to transfer custody of the information to a different data owner.
8.Create a procedure to periodically review the classification and ownership. Communicate any changes to the data custodian.
9.Indicate termination procedures for declassifying the data.
10.
Integrate these issues into the security-awareness program so that all employees understand how to handle data at different classification levels.
Domain: Information security and risk management
Reference: AIO 3rd edition page 50

NEW QUESTION: 645
Which of the following statements regarding an off-site information processing facility is TRUE?
A. It should have the same amount of physical access restrictions as the primary processing site.
B. It should be located in proximity to the originating site so that it can quickly be made operational.
C. It should be easily identified from the outside so in the event of an emergency it can be easily found.
D. Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.
Answer: (SHOW ANSWER)
Explanation/Reference:
It is very important that the offsite has the same restrictions in order to avoide misuse.
The following answers are incorrect because:
It should be located in proximity to the originating site so that it can quickly be made operational is incorrect as the offsite is also subject to the same disaster as of the primary site.
It should be easily identified from the outside so in the event of an emergency it can be easily found is also incorrect as it should not be easily identified to prevent intentional sabotage.
Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive is also incorrect as it should be like its primary site.
Reference : Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 265).

NEW QUESTION: 646
Which of the following algorithms does NOT provide hashing?
A. SHA-1
B. MD2
C. RC4
D. MD5
Answer: (SHOW ANSWER)
Explanation/Reference:

As it is an algorithm used for encryption and does not provide hashing functions , it is also commonly implemented ' Stream Ciphers '.
The other answers are incorrect because :
SHA-1 was designed by NIST and NSA to be used with the Digital Signature Standard (DSS). SHA was designed to be used in digital signatures and was developed when a more secure hashing algorithm was required for U.S. government applications.
MD2 is a one-way hash function designed by Ron Rivest that creates a 128-bit message digest value. It is not necessarily any weaker than the other algorithms in the "MD" family, but it is much slower.
MD5 was also created by Ron Rivest and is the newer version of MD4. It still produces a 128-bit hash, but the algorithm is more complex, which makes it harder to break.
Reference : Shon Harris , AIO v3 , Chapter - 8 : Cryptography , Page : 644 - 645

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam!
BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here:
https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps,
40%OFF Special Discount: Exam-Tests)

NEW QUESTION: 647
Access Control techniques do not include which of the following choices?
A. Relevant Access Controls
B. Discretionary Access Control
C. Mandatory Access Control
D. Lattice Based Access Control
Answer: (SHOW ANSWER)
Section: Access Control
Explanation/Reference:
Access Control Techniques
Discretionary Access Control
Mandatory Access Control
Lattice Based Access Control
Rule-Based Access Control
Role-Based Access Control
Source: DUPUIS, Clement, Access Control Systems and Methodology, Version 1, May 2002, CISSP Open Study Group Study Guide for Domain 1, Page 13.

NEW QUESTION: 648
A boot sector virus goes to work when what event takes place?

A. March 16th
B. File is saved
C. Reboot or system startup
D. File is deleted
Answer: C (LEAVE A REPLY)

NEW QUESTION: 649
Which of the following best defines a Computer Security Incident Response Team (CSIRT)?
A. An organization that provides a secure channel for receiving reports about suspected security incidents.
B. An organization that ensures that security incidents are reported to the authorities.
C. An organization that coordinates and supports the response to security incidents.
D. An organization that disseminates incident-related information to its constituency and other involved parties.
Answer: C (LEAVE A REPLY)
Section: Risk, Response and Recovery
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines a Computer Security Incident Response Team (CSIRT) as an organization that coordinates and supports the response to security incidents that involves sites within a defined constituency. This is the proper definition for the CSIRT. To be considered a CSIRT, an organization must provide a secure channel for receiving reports about suspected security incidents, provide assistance to members of its constituency in handling the incidents and disseminate incident-related information to its constituency and other involved parties. Security-related incidents do not necessarily have to be reported to the authorities.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION: 650
A DMZ is also known as a
A. screened subnet
B. three legged firewall
C. a place to attract hackers
D. bastion host
Answer: (SHOW ANSWER)
Explanation/Reference:
This is another name for the demilitarized zone (DMZ) of a network.
"Three legged firewall" is incorrect. While a DMZ can be implemented on one leg of such a device, this is not the best answer.
"A place to attract hackers" is incorrect. The DMZ is a way to provide limited public access to an organization's internal resources (DNS, EMAIL, public web, etc) not as an attractant for hackers.
"Bastion host" is incorrect. A bastion host serves as a gateway between trusted and untrusted network.
References:

CBK, p. 434
AIO3, pp. 495 - 496

NEW QUESTION: 651
What is NOT an authentication method within IKE and IPsec?
A. CHAP
B. Pre shared key
C. certificate based authentication
D. Public key authentication
Answer: (SHOW ANSWER)
Explanation/Reference:
CHAP is not used within IPSEC or IKE. CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password).
After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.
The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.
The following were incorrect answers:
Pre Shared Keys
In cryptography, a pre-shared key or PSK is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. To build a key from shared secret, the key derivation function should be used. Such systems almost always use symmetric key cryptographic algorithms. The term PSK is used in WiFi encryption such as WEP or WPA, where both the wireless access points (AP) and all clients share the same key.
The characteristics of this secret or key are determined by the system which uses it; some system designs require that such keys be in a particular format. It can be a password like 'bret13i', a passphrase like 'Idaho hung gear id gene', or a hexadecimal string like '65E4 E556 8622 EEE1'. The secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems.
Certificat Based Authentication
The most common form of trusted authentication between parties in the wide world of Web commerce is the exchange of certificates. A certificate is a digital document that at a minimum includes a Distinguished Name (DN) and an associated public key.
The certificate is digitally signed by a trusted third party known as the Certificate Authority (CA). The CA vouches for the authenticity of the certificate holder. Each principal in the transaction presents certificate

as its credentials. The recipient then validates the certificate's signature against its cache of known and trusted CA certificates. A "personal
certificate" identifies an end user in a transaction; a "server certificate" identifies the service provider. Generally, certificate formats follow the X.509 Version 3 standard. X.509 is part of the Open Systems Interconnect
(OSI) X.500 specification.
Public Key Authentication
Public key authentication is an alternative means of identifying yourself to a login server, instead of typing a password. It is more secure and more flexible, but more difficult to set up.
In conventional password authentication, you prove you are who you claim to be by proving that you know the correct password. The only way to prove you know the password is to tell the server what you think the password is. This means that if the server has been hacked, or spoofed an attacker can learn your password.
Public key authentication solves this problem. You generate a key pair, consisting of a public key (which everybody is allowed to know) and a private key (which you keep secret and do not give to anybody). The private key is able to generate signatures. A signature created using your private key cannot be forged by anybody who does not have a copy of that private key; but anybody who has your public key can verify that a particular signature is genuine.
So you generate a key pair on your own computer, and you copy the public key to the server. Then, when the server asks you to prove who you are, you can generate a signature using your private key. The server can verify that signature (since it has your public key) and allow you to log in. Now if the server is hacked or spoofed, the attacker does not gain your private key or password; they only gain one signature. And signatures cannot be re-used, so they have gained nothing.
There is a problem with this: if your private key is stored unprotected on your own computer, then anybody who gains access to your computer will be able to generate signatures as if they were you. So they will be able to log in to your server under your account. For this reason, your private key is usually encrypted when it is stored on your local machine, using a passphrase of your choice. In order to generate a signature, you must decrypt the key, so you have to type your passphrase.
References:
RFC 2409: The Internet Key Exchange (IKE); DORASWAMY, Naganand & HARKINS, Dan Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 1999, Prentice Hall PTR; SMITH, Richard E.
Internet Cryptography, 1997, Addison-Wesley Pub Co.; HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 467.
http://en.wikipedia.org/wiki/Pre-shared_key
http://www.home.umk.pl/~mgw/LDAP/RS.C4.JUN.97.pdf
http://the.earth.li/~sgtatham/putty/0.55/htmldoc/Chapter8.html#S8.1

NEW QUESTION: 652
Which of the following are required for Life-Cycle Assurance?
A. System Architecture and Design specification.

B. Security Testing and Covert Channel Analysis.
C. Security Testing and Trusted distribution.
D. Configuration Management and Trusted Facility Management.
Answer: C (LEAVE A REPLY)
Section: Security Operation Adimnistration
Explanation/Reference:
Security testing and trusted distribution are required for Life-Cycle Assurance.
The following answers are incorrect:
System Architecture and Design specification. Is incorrect because System Architecture is not requried for Life- Cycle Assurance.
Security Testing and Covert Channel Analysis. Is incorrect because Covert Channel Analysis is not requried for Life-Cycle Assurance.
Configuration Management and Trusted Facility Management. Is incorrect because Trusted Facility Management. is not requried for Life-Cycle Assurance.

NEW QUESTION: 653
Which of the following statements pertaining to access control is false?
A. Users should only access data on a need-to-know basis.
B. If access is not explicitly denied, it should be implicitly allowed.
C. Access rights should be granted based on the level of trust a company has on a subject.
D. Roles can be an efficient way to assign rights to a type of user who performs certain tasks.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Access control mechanisms should default to no access to provide the necessary level of security and ensure that no security holes go unnoticed. If access is not explicitly allowed, it should be implicitly denied.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter
4: Access Control (page 143).

NEW QUESTION: 654
Which of the following security-focused protocols has confidentiality services operating at a layer different from the others?
A. Secure HTTP (S-HTTP)
B. FTP Secure (FTPS)
C. Secure socket layer (SSL)
D. Sequenced Packet Exchange (SPX)
Answer: A (LEAVE A REPLY)
Section: Network and Telecommunications
Explanation/Reference:

All the previous protocols operate at the transport layer except for Secure HTTP (S-HTTP), which operates at the application layer. S-HTTP has been replaced by SSL and TLS.
As it is very well explained in the Shon Harris book:
The transport layer receives data from many different applications and assembles the data into a stream to be properly transmitted over the network. The main protocols that work at this layer are TCP, UDP, Secure Sockets Layer (SSL), and Sequenced Packet Exchange (SPX).
NOTE:
Different references can place specific protocols at different layers. For example, many references place the SSL protocol in the session layer, while other references place it in the transport layer. It is not that one is right or wrong. The OSI model tries to draw boxes around reality, but some protocols straddle the different layers.
SSL is made up of two protocols- one works in the lower portion of the session layer and the other works in the transport layer.
For purposes of the CISSP exam, SSL resides in the transport layer.
Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 526). McGraw-Hill. Kindle Edition.

NEW QUESTION: 655
Which of the following is not a logical control when implementing logical access security?
A. access profiles.
B. userids.
C. employee badges.
D. passwords.
Answer: (SHOW ANSWER)
Employee badges are considered Physical so would not be a logical control.
The following answers are incorrect:
userids. Is incorrect because userids are a type of logical control. access profiles. Is incorrect because access profiles are a type of logical control. passwords. Is incorrect because passwords are a type of logical control.

NEW QUESTION: 656
Each data packet is assigned the IP address of the sender and the IP address of the:
A. recipient.
B. host.
C. node.
D. network.
Answer: A (LEAVE A REPLY)
Each data packet is assigned the IP address of the sender and the IP address of the recipient. The term network refers to the part of the IP address that identifies each network. The terms host and node refer to the parts of the IP address that identify a specific machine on a network.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

NEW QUESTION: 657
In stateful inspection firewalls, packets are:
A. Inspected at only one layer of the Open System Interconnection (OSI) model
B. Inspected at all Open System Interconnection (OSI) layers
C. Decapsulated at all Open Systems Interconnect (OSI) layers.
D. Encapsulated at all Open Systems Interconnect (OSI) layers.
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Many times when a connection is opened, the firewall will inspect all layers of the packet. While this inspection is scaled back for subsequent packets to improve performance, this is the best of the four answers.
When packet filtering is used, a packet arrives at the firewall, and it runs through its ACLs to determine whether this packet should be allowed or denied. If the packet is allowed, it is passed on to the destination host, or to another network device, and the packet filtering device forgets about the packet. This is different from stateful inspection, which remembers and keeps track of what packets went where until each particular connection is closed. A stateful firewall is like a nosy neighbor who gets into people's business and conversations. She keeps track of the suspicious cars that come into the neighborhood, who is out of town for the week, and the postman who stays a little too long at the neighbor lady's house. This can be annoying until your house is burglarized. Then you and the police will want to talk to the nosy neighbor, because she knows everything going on in the neighborhood and would be the one most likely to know something unusual happened.
"Inspected at only one Open Systems Interconnetion (OSI) layer" is incorrect. To perform stateful packet inspection, the firewall must consider at least the network and transport layers.
"Decapsulated at all Open Systems Interconnection (OSI) layers" is incorrect. The headers are not stripped ("decapsulated" if there is such a word) and are passed through in their entirety IF the packet is passed.
"Encapsulated at all Open Systems Interconnect (OSI) layers" is incorrect. Encapsulation refers to the adding of a layer's header/trailer to the information received from the above level. This is done when the packet is assembled not at the firewall.
Reference(s) used for this question:
CBK, p. 466
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 632-633). McGraw-Hill. Kindle Edition.

Valid SSCP Dumps shared by BraindumpsPass.com for Helping Passing SSCP Exam! BraindumpsPass.com now offer the **newest SSCP exam dumps**, the BraindumpsPass.com SSCP

exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com SSCP dumps with Test Engine here: https://www.braindumpspass.com/ISC/SSCP-practice-exam-dumps.html (**1338** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)