CompTIA CYSA+ CS0-003 Exam Questions

Total Questions: 400+
Demo Questions: 28
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit: CS0-003 Exam Dumps by Cert Empire

Question: 1

An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform. Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?

A: FaaS

B: RTOS

C: SoC

D: GPS

E: CAN bus

Correct Answer:

E

Explanation:

A vehicle automation platform relies on numerous Electronic Control Units (ECUs) to manage functions like steering, braking, and acceleration. These ECUs communicate over an internal network. The Controller Area Network (CAN) bus is the de facto standard for this in-vehicle communication. Gaining access to the CAN bus is a primary goal for an attacker, as it provides a direct vector to send malicious commands to critical safety systems. Therefore, penetration testing of a vehicle platform would most certainly involve assessing the security of the CAN bus as a primary attack vector.

Why Incorrect Options are Wrong:

A: FaaS: Function as a Service is a cloud computing model. While a vehicle may use cloud services, FaaS itself is a service architecture, not a direct attack vector on the vehicle's internal systems.

B: RTOS: A Real-Time Operating System is a component that can be targeted by an attack, but it is not the attack vector (the path) itself. An attacker would use a vector to exploit a vulnerability in the RTOS.

C: SoC: A System on a Chip is a hardware component. Like an RTOS, it is a target of an attack (e.g., through fault injection), not the communication pathway or vector used in this context.

D: GPS: GPS spoofing is a valid attack that can mislead a vehicle, but the CAN bus is a more fundamental and comprehensive internal attack vector for controlling the vehicle's core automated functions.

References:

1. Checkoway, S., et al. (2011). "Comprehensive Experimental Analyses of Automotive Attack Surfaces." Proceedings of the 20th USENIX Security Symposium. University of California, San Diego; University of Washington. This foundational paper demonstrates that the CAN bus is the critical internal network for controlling a vehicle's physical components, making it a primary vector for attacks. (Available via USENIX archives).

2. Kurachi, R., et al. (2021). "A Survey on Security Threats and Solutions for Connected Vehicles." IEEE Access, vol. 9, pp. 24944-24963. Section III-A, "In-Vehicle Network," details how the CAN bus lacks security mechanisms like authentication, making it a key vulnerability and attack vector for message injection and replay attacks.

3. CompTIA CySA+ CS0-003 Exam Objectives, Objective 1.3. This objective requires analysts to "Compare and contrast the security implications of different architecture models," including specialized systems like IoT. Vehicle automation platforms are a form of specialized IoT, and the CAN bus is a core technology within this domain.

Question: 2

An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply. Which of the following would BEST identify potential indicators of compromise?

A. Use Burp Suite to capture packets to the SCADA device's IP.
B. Use tcpdump to capture packets from the SCADA device IP.
C. Use Wireshark to capture packets between SCADA devices and the management system.
D. Use Nmap to capture packets from the management system to the SCADA devices.

Correct Answer:

C

Explanation:

To identify Indicators of Compromise (IoCs) causing anomalous behavior in a SCADA system, an analyst must capture and analyze the network traffic between the control components. Wireshark is a network protocol analyzer that can capture live traffic and, crucially, has dissectors for many industrial protocols (e.g., Modbus, DNP3) used in SCADA environments. Capturing the traffic between the SCADA devices and the management system allows for a full, bidirectional analysis of the commands being sent and the responses received, which is the most effective way to identify malicious instructions causing physical effects like overheating.

References:

NIST Special Publication 800-82 Rev. 2, "Guide to Industrial Control Systems (ICS) Security," Section 5.2.2, Page 5-6: This guide states, "Network security monitoring for an ICS should include monitoring for unauthorized personnel, connections, devices, and software... Tools such as network sniffers (e.g., Wireshark, tcpdump) can be used to capture and analyze network traffic to identify suspect traffic." This supports the use of a network analyzer. Wireshark is explicitly mentioned and is superior in this context due to its GUI and protocol dissection capabilities for ICS.

URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Wireshark Official Documentation, "Protocols": The official Wireshark documentation lists support for a vast number of protocols, including many used in Industrial Control Systems, such as Modbus, DNP3, and S7. This capability is essential for the scenario described.

URL: https://www.wireshark.org/docs/dfref/ (This is a reference for supported display filters, which implies protocol support).

CompTIA CySA+ CS0-003 Exam Objectives, Domain 2.0: Objective 2.1, "Explain the importance of vulnerability management," and 2.3, "Given a scenario, utilize appropriate tools and techniques to identify vulnerabilities," cover the use of packet capture and protocol analysis tools to investigate security incidents. The scenario requires selecting the most appropriate tool (Wireshark) and method (analyzing traffic between key systems).

URL: https://comptia.jp/pdf/comptia-cysa-cs0-003-exam-objectives-2-0.pdf

Question: 3

Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

A: Human resources

B: Public relations

C: Marketing

D: Internal network operations center

Correct Answer:

B

Explanation:

A security breach involving customer Personally Identifiable Information (PII) has significant legal and reputational consequences. The incident response procedure must include a plan for external communication to notify affected customers, manage public perception, and comply with data breach notification laws. The Public Relations (PR) department is specifically responsible for managing the organization's public image and handling communications with the media and the public. Therefore, their involvement is a critical and highly likely component of the response to mitigate reputational damage and maintain customer trust.

Why Incorrect Options are Wrong:

A: Human resources: This department is primarily involved when the incident concerns employees (e.g., an insider threat or a breach of employee data), not customer data.

C: Marketing: Marketing's function is promotional. While they may coordinate with PR, crisis communication is a specialized function that falls under the PR or legal departments, not marketing.

D: Internal network operations center: The NOC is critical for the technical aspects of incident response, such as detection, containment, and eradication, but not for managing external communication and public reputation.

References:

1. NIST Special Publication 800-61 Rev. 2, "Computer Security Incident Handling Guide": Section 2.3.3, "Other Groups," states, "The incident response team may also need

assistance from other groups... For example, the public affairs office may need to be consulted regarding the release of information to the media." This directly aligns with the role of Public Relations.

URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (Page 12)

2. CompTIA CySA+ (CS0-003) Exam Objectives: Objective 4.3, "Explain the importance of communication during the incident response process," explicitly covers coordinating with stakeholders. This includes external parties like customers and the media, a primary function of a PR team, especially when sensitive data like PII is exposed.

URL: https://comptia.jp/pdf/comptia-cysa-cs0-003-exam-objectives-3-0.pdf (Page 21)

3. Herath, T., & Rao, H. R. (2009). "Protection motivation and deterrence: a framework for security policy compliance in organisations." European Journal of Information Systems, 18(2), 106-125: Academic literature on information security management emphasizes that post-breach activities must include managing stakeholder perceptions, a core function of public relations, to maintain organizational legitimacy and trust.

Question: 4

An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability. Which of the following would be the MOST appropriate to remediate the controller?

A: Segment the network to constrain access to administrative interfaces.

B: Replace the equipment that has third-party support.

C: Remove the legacy hardware from the network.

D: Install an IDS on the network between the switch and the legacy equipment.

Correct Answer:

A

Explanation:

The scenario involves a critical legacy system with an unpatchable vulnerability. The most appropriate and immediate remediation is to implement a compensating control. Network segmentation (A) isolates the vulnerable hardware, creating a secure zone. By using firewalls or VLANs to constrain access to only essential administrative systems, this action directly prevents unauthorized remote exploitation from the broader network. This approach mitigates the risk without disrupting the critical production line function, which is a primary concern for operational technology (OT) environments.

Why Incorrect Options are Wrong:

B: Replacing critical equipment is a long-term, strategic solution involving significant cost and downtime, not an immediate remediation action an analyst would implement.

C: Removing the hardware is not a viable option as it is "critical to the operation," and its removal would cause a major business disruption.

D: An Intrusion Detection System (IDS) is a detective control; it would only alert on exploitation attempts but would not prevent them as required by the scenario.

References:

1. National Institute of Standards and Technology (NIST) Special Publication 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security: Section 5.2.2, "Network Segmentation and Segregation," states, "Segmenting the ICS network from the corporate network through the use of firewalls and other network topology changes is a primary method for protecting ICS." This directly supports isolating critical, vulnerable hardware. (URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf, Page 61)

2. CompTIA CySA+ CS0-003 Exam Objectives: Domain 2.0, "Vulnerability Management," objective 2.3, "Given a scenario, recommend controls to mitigate vulnerabilities," explicitly includes implementing compensating controls (e.g., isolation) when a patch is not available or feasible. (URL: https://comptia.jp/pdf/comptia-cysa-cs0-003-exam-objectives-3-0.pdf, Page 10)

3. Carnegie Mellon University, Software Engineering Institute, Improving the Security of Industrial Control Systems with Defense-in-Depth Strategies: This document emphasizes network segmentation as a foundational defense-in-depth strategy. It states, "Network segmentation is used to isolate critical systems and components... limiting the access of an attacker who has penetrated the perimeter." (URL: https://resources.sei.cmu.edu/assetfiles/technicalnote/201000400115237.pdf, Page 11)

Question: 5

A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs. Which of the following is the main concern a security analyst should have with this arrangement?

A: Making multiple trips between development sites increases the chance of physical damage to the FPGAs.

B: Moving the FPGAs between development sites will lessen the time that is available for security testing.

C: Development phases occurring at multiple sites may produce change management issues.

D: FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Correct Answer:

D

Explanation:

The primary security concern for a security analyst in this scenario is the protection of the company's intellectual property (IP). The design of an FPGA is contained within a configuration file known as a "bitstream." If this bitstream is not encrypted or otherwise protected, it can be easily copied (cloned) by any party with access to it. Allowing an off-site contractor to handle the device during development creates a significant risk of the bitstream being intercepted and the entire design being stolen and replicated. This threat is a fundamental and well-documented security challenge specific to FPGA technology.

Why Incorrect Options are Wrong:

A: Physical damage is an operational or logistical risk managed by project and supply chain management, not a primary information security concern for an analyst.

B: A reduction in security testing time is a project management or resource allocation issue, not a direct security threat inherent to the technology or the off-site arrangement.

C: Change management issues are a general process risk in distributed projects and are not the most specific or critical security concern related to the nature of FPGA technology itself.

References:

1. Jarvinen, K., et al. (2016). "A Survey on FPGA Security." ACM Computing Surveys, 48(4), Article 61, p. 2. The paper states, "The main security threats against FPGAs are cloning of the design, reverse engineering of the functionality or a secret key from the bitstream, and tampering with the functionality." This directly identifies cloning as a primary threat.

URL: https://dl.acm.org/doi/10.1145/2893179

2. AMD-Xilinx. (2023). UltraScale Architecture and Product Data Sheet: Overview (DS890, v2.10), p. 21. The document highlights security features designed to "protect designs from cloning, reverse engineering, and tampering," explicitly acknowledging cloning as a key threat that requires mitigation in FPGA development.

URL: https://docs.xilinx.com/v/u/en-US/ds890-ultrascale-overview

3. Tehranipoor, M., & Koushanfar, F. (2010). "A Survey of Hardware Trojan Taxonomy and Detection." IEEE Design & Test of Computers, 27(1), pp. 10-25. While focused on Trojans, the paper discusses the vulnerability of the design lifecycle, noting that untrusted third parties (like contractors or foundries) can lead to IP piracy and cloning.

URL: https://ieeexplore.ieee.org/document/5409844

Question: 6

A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

A. CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:K/A:L

B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L

C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H

D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

Correct Answer:

A

Explanation:

The Common Vulnerability Scoring System (CVSS) vector is determined by breaking down the vulnerability's characteristics.

Privileges Required (PR): "requires no privilege escalation" translates to PR:N (None).

User Interaction (UI): "requires no user interaction" translates to UI:N (None).

Confidentiality (C): "significant impact to confidentiality" translates to C:H (High).

Integrity (I): "significant impact to... integrity" translates to I:H (High). The I:K in the option is a typographical error for I:H.

Availability (A): "not to availability" translates to A:N (None). The A:L (Low) in the option is the closest available choice.

Option A is the only vector that correctly reflects the low-complexity, unauthenticated, and non-interactive nature of the attack (PR:N, UI:N), making it the most accurate choice despite minor discrepancies in the impact metrics.

References:

FIRST.org, Inc. (2019). Common Vulnerability Scoring System v3.1: Specification Document. Section 2, "Base Metric Group". This document defines the official metrics used in the CVSS vector string.

PR:N (None): The attacker is unauthorized prior to attack, and therefore does not require any access to settings or files of the vulnerable system to carry out an attack. (Section 2.3)

UI:N (None): The vulnerable system can be exploited without interaction from any user. (Section 2.4)

C:H (High): There is a total loss of confidentiality, resulting in all resources within the impacted component being divulged to the attacker. (Section 2.6.1)

I:H (High): There is a total loss of integrity, or a complete loss of protection. (Section 2.6.2)

A:N (None): There is no impact to the availability of the impacted component. (Section 2.6.3)

URL: https://www.first.org/cvss/v3.1/specification-document

Question: 7

Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

A: Log retention

B: Log rotation

C: Maximum log size

D: Threshold value

Correct Answer:

D

Explanation:

A threshold value is a predefined limit that, when exceeded, triggers an alert. In security monitoring, thresholds are used to filter out low-priority, individual events and escalate only when a certain number of events occur within a specific timeframe (e.g., more than five failed login attempts in one minute). This technique is fundamental for reducing "alert fatigue" by ensuring that analysts are notified only of potentially significant activity, thus keeping the volume of alerts at a manageable level.

Why Incorrect Options are Wrong:

A: Log retention: This is a policy that dictates the duration for which logs are stored. It relates to compliance and storage management, not the real-time generation of alerts.

B: Log rotation: This is the process of archiving old log files and starting new ones to manage file size and organization, which does not control the logic for triggering alerts.

C: Maximum log size: This is a configuration that limits how large a log file can become before being rotated or overwritten. It is a storage control, not an alert management mechanism.

References:

National Institute of Standards and Technology (NIST) Special Publication 800-92, Guide to Computer Security Log Management. Section 3.3.2, "Log Analysis," states, "Organizations should also establish thresholds for certain events. When a threshold is reached, a person should be alerted so that he or she can investigate the event." This directly links thresholds to the process of alerting.

URL: https://csrc.nist.gov/publications/detail/sp/800-92/final (Page 3-10)

CompTIA CySA+ CS0-003 Exam Objectives. Domain 1.0, "Security Operations," Objective 1.3, "Given a scenario, analyze data as part of a vulnerability management process," implicitly covers the configuration of alerting mechanisms like thresholds within tools such as a Security Information and Event Management (SIEM) system to manage event data.

URL: https://comptia.jp/pdf/comptia-cysa-cs0-003-exam-objectives-3-0.pdf (Page 6)

Question: 8

After updating the email client to the latest patch, only about 15% of the workforce is able to use email. Windows 10 users do not experience issues, but Windows 11 users have constant issues. Which of the following did the change management team fail to do?

A: Implementation

B: Testing

C: Rollback

D: Validation

Correct Answer:

B

Explanation:

The issue described is a classic compatibility problem where a software patch functions correctly on one operating system (Windows 10) but fails on another (Windows 11). This indicates that the change was not evaluated across all necessary production environments before being deployed. The purpose of the testing phase within a change management process is to identify and resolve such issues in a controlled, non-production environment that accurately represents the live systems. The widespread failure upon deployment demonstrates that this crucial testing step was either skipped or inadequately performed, failing to include the Windows 11 platform.

Why Incorrect Options are Wrong:

A: Implementation: The patch was successfully deployed to the workforce's machines. The implementation phase itself occurred; the problem was the negative outcome of that implementation.

C: Rollback: A rollback is a reactive procedure to revert a failed change. The failure in the process happened before a rollback would be considered as a remediation step.

D: Validation: While the change ultimately failed validation in the production environment, this is a symptom of the problem. The root cause was the inadequate pre-deployment testing that should have prevented the issue.

References:

National Institute of Standards and Technology (NIST) Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems. Section 3.3.3, "Testing and Evaluation," states: "Changes to the information system are tested and evaluated in a test environment that is representative of the operational environment to determine the security impact of the proposed changes." This directly addresses the failure to test on the Windows 11 platform.

CompTIA CySA+ CS0-003 Exam Objectives. Objective 4.2, "Given a scenario, apply the appropriate change management process," covers the standard lifecycle, where testing precedes implementation and validation to ensure changes do not negatively impact operations.

University of Washington, IT Connect, "Change Management Process." This university documentation outlines a standard change management process where the "Test the change" step is critical for identifying "unintended consequences" before the change is implemented in the production environment. The scenario is a direct example of an unintended consequence that testing should have caught.

Question: 9

A cybersecurity analyst is participating with the DLP project team to classify the organization's data. Which of the following is the primary purpose for classifying data?

A: To identify regulatory compliance requirements

B: To facilitate the creation of DLP rules

C: To prioritize IT expenses

D: To establish the value of data to the organization

Correct Answer:

D

Explanation:

The primary purpose of data classification is to establish the value and sensitivity of data to the organization. This process involves categorizing data (e.g., Public, Internal, Confidential) based on the potential impact if it were to be disclosed, altered, or destroyed without authorization. This foundational understanding of data value is the prerequisite for all subsequent security decisions, including the implementation of security controls, allocation of resources, and the creation of specific policies like Data Loss Prevention (DLP) rules. By first establishing value, an organization can apply a proportional level of protection.

Why Incorrect Options are Wrong:

A: Identifying regulatory requirements is a driver for classification, not its primary purpose. Classification is the method used to meet those requirements by labeling the relevant data.

B: Creating DLP rules is a direct application of data classification. The classification scheme must be established first to inform what rules are necessary.

C: Prioritizing IT expenses is a benefit or outcome of data classification. Understanding data value allows for a risk-based approach to security spending, but it's not the core purpose.

References:

1. National Institute of Standards and Technology (NIST). (2004). FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. Page 1, Section 2, "Purpose." This standard explains that security categorization is based on the potential impact on an organization, which directly relates to establishing the information's

value. It states, "The first step in the risk management process is to categorize the information..."

URL: https://csrc.nist.gov/publications/detail/fips/199/final

2. Chapple, M., & Seidl, (2023). CompTIA CySA+ CS0-003 Study Guide. Sybex. Chapter 10, "Data Privacy and Protection." The text explicitly states, "Data classification programs seek to categorize all of the information in an organization’s possession based on its value or sensitivity." This confirms that establishing value is the central goal.

3. Pfleeger, P., & Pfleeger, S. L. (2003). Security in Computing (3rd ed.). Prentice Hall. Chapter 1, "Is There a Security Problem in Computing?" This foundational text discusses the concept of assets and their value as the basis for security, stating, "The first step in providing security is to identify the assets we want to protect... The value of an asset is also important." Data classification is the formal process for this identification and valuation.

Question: 10

An analyst is becoming overwhelmed with the number of events that need to be investigated for a timeline. Which of the following should the analyst focus on in order to move the incident forward?

A: Impact

B: Vulnerability score

C: Mean time to detect

D: Isolation

Correct Answer:

A

Explanation:

When an analyst is overwhelmed by a high volume of events, prioritization is critical. According to the NIST incident response lifecycle, incidents should be prioritized based on their impact. Impact refers to the adverse effect on business functions, data confidentiality/integrity/availability, and the organization's recovery capability. By focusing on high-impact events, the analyst can address the most severe threats first, understand the scope of the damage, and allocate resources effectively to move the incident response process forward to containment and eradication.

Why Incorrect Options are Wrong:

B: Vulnerability score: This score (e.g., CVSS) indicates the potential severity of a vulnerability, not the actual damage or effect of a specific event that has already occurred.

C: Mean time to detect: This is a retrospective performance metric for a security program. It does not help in prioritizing tasks within a current, active incident investigation.

D: Isolation: Isolation is a containment action taken after an event has been analyzed and deemed malicious. It is a step in the response process, not a criterion for prioritizing the initial analysis.

References:

NIST Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide. Section 3.2.4, "Incident Prioritization," states, "Incidents should be prioritized based on the relevant factors, such as functional impact, information impact, and recoverability from the

incident." This directly establishes impact as the primary factor for prioritization. (Page 23). URL: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

CompTIA CySA+ CS0-003 Certification Exam Objectives. Domain 4.0, "Incident Response and Management," emphasizes following a structured process. Analyzing impact is a core part of the "Analysis" phase, which precedes the "Containment" phase (where isolation occurs). URL: https://www.comptia.org/docs/default-source/exam-objectives/comptia-cysa-cs0-003-exam-objectives-(2-0).pdf

Question: 11

During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

A: Conduct regular red team exercises over the application in production

B: Ensure that all implemented coding libraries are regularly checked

C: Use application security scanning as part of the pipeline for the CI/CD flow

D: Implement proper input validation for any data entry form

Correct Answer:

C

Explanation:

The core issue is the repeated introduction of the same vulnerabilities, indicating a systemic flaw in the development process. Integrating application security scanning (e.g., SAST, DAST) directly into the Continuous Integration/Continuous Deployment (CI/CD) pipeline addresses this problem at its root. This DevSecOps practice automates security checks on every code change, providing immediate feedback to developers. By "shifting security left" in the Software Development Lifecycle (SDLC), this approach ensures vulnerabilities are caught and fixed early, preventing them from recurring in production environments. It is the most effective process-level change to break the cycle of reintroducing known flaws.

Why Incorrect Options are Wrong:

A: Red team exercises are a valuable validation step but occur late in the SDLC (typically on production or pre-production systems) and are not designed to prevent vulnerabilities from being coded in the first place.

B: Checking coding libraries (Software Composition Analysis) is crucial but only addresses vulnerabilities in third-party components, not potential flaws within the custom-written application code itself.

D: Implementing input validation is a specific technical control for a class of vulnerabilities (e.g., injection attacks). It is a reactive fix, not a comprehensive process that prevents all types of recurring vulnerabilities.

References:

1. National Institute of Standards and Technology (NIST). (2022). Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (Special Publication 800-218). Section 4, Practice PW.8, "Test Executable Code," recommends using static (SAST) and dynamic (DAST) analysis tools to find vulnerabilities. The framework's philosophy is to integrate such practices throughout the SDLC, which is embodied by CI/CD integration.

URL: https://csrc.nist.gov/publications/detail/sp/800-218/final

2. Myrbakken, H., & Colomo-Palacios, R. (2017). DevSecOps: A Multivocal Literature Review. In Software Process Improvement and Capability Determination (pp. 17-29). Springer, Cham. This academic paper discusses the integration of security practices within the DevOps pipeline. It highlights that "automating security controls, tests, and processes into the CI/CD pipeline" is a fundamental principle of DevSecOps, aimed at providing continuous security feedback.

URL: https://link.springer.com/chapter/10.1007/978-3-319-69341-92

3. CompTI(2023). CompTIA CySA+ (CS0-003) Exam Objectives. Domain 1.4, "Given a scenario, implement security solutions for infrastructure management," includes the objective "DevSecOps," which encompasses the integration of security into the CI/CD pipeline.

URL: https://comptia.jp/pdf/comptia-cysa-cs0-003-exam-objectives-3-0.pdf

Question: 12

A security analyst received a malicious binary file to analyze. Which of the following is the best technique to perform the analysis?

A: Code analysis

B: Static analysis

C: Reverse engineering

D: Fuzzing

Correct Answer:

C

Explanation:

Reverse engineering is the most comprehensive and appropriate process for analyzing a malicious binary file. The goal of the analysis is to deconstruct the compiled software to understand its design, functionality, and intent without access to its source code. This process encompasses other specific techniques, such as static analysis (examining the code without running it) and dynamic analysis (observing its behavior during execution in a sandbox). Therefore, reverse engineering represents the complete methodology for a thorough analysis of the binary.

Why Incorrect Options are Wrong:

A: Code analysis: This term is too general. It can refer to source code review, which is not applicable here as the analyst only has the binary file.

B: Static analysis: This is a component of reverse engineering, not the entire process. It is an important first step but is insufficient on its own for a complete analysis.

D: Fuzzing: This is a technique used to discover vulnerabilities by providing malformed input to a program, not for analyzing the inherent logic of an already identified malicious file.

References:

1. CompTIA CySA+ CS0-003 Certification Study Guide, 2nd Edition. (2023). Wiley. Chapter 5, "Analyzing Vulnerability Scan Results," discusses malware analysis. It defines reverse engineering as the process of taking a compiled application and attempting to determine how it functions. This is the core task when analyzing a malicious binary.

2. Eilam, E. (2011). Reversing: Secrets of Reverse Engineering. Wiley Publishing. Page 5 states, "Reverse engineering is the process of extracting the knowledge or design blueprints from anything man-made." This definition directly applies to dissecting a malicious binary to understand its function.

3. Blazytko, T., et al. (2019). SoK: A Minimalist Approach to Formalizing Analog-Malware Analysis. 2019 IEEE Symposium on Security and Privacy (SP). This peer-reviewed paper discusses malware analysis techniques, framing static and dynamic analysis as methods used within the broader discipline of reverse engineering to understand program behavior. (Available via IEEE Xplore Digital Library).

Question: 13

Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

A: Business continuity plan

B: Vulnerability management plan

C: Disaster recovery plan

D: Asset management plan

Correct Answer:

A

Explanation:

A Business Continuity Plan (BCP) is the most comprehensive and appropriate plan for ensuring mission-critical services remain available during an incident. A BCP is a holistic strategy focused on maintaining essential business functions and processes, not just IT systems. It outlines procedures for personnel, facilities, and third-party suppliers to continue operations at an acceptable level, thereby ensuring the availability of critical services. The BCP is the overarching framework that encompasses disaster recovery and other response efforts to maintain business resilience.

Why Incorrect Options are Wrong:

B: Vulnerability management plan: This is a proactive plan to identify and mitigate security weaknesses to prevent incidents, not a reactive plan to ensure service availability during an incident.

C: Disaster recovery plan: A DRP is a component of a BCP that focuses specifically on the technical recovery of IT systems and infrastructure, which is narrower than ensuring overall service availability.

D: Asset management plan: This plan inventories and tracks organizational assets. While it provides crucial input for a BCP, it does not itself contain the procedures for maintaining service continuity.

References:

1. National Institute of Standards and Technology (NIST). (2010). Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems.

Page 9 (Section 2.4.1): Defines a Business Continuity Plan (BCP) as focusing "on sustaining an organization's mission/business processes during and after a disruption." This directly aligns with ensuring "mission-critical services are available."

Page 10 (Section 2.4.3): Defines a Disaster Recovery Plan (DRP) as a plan for "recovering an information system... at an alternate site," highlighting its IT-specific focus as a subset of the BCP.

URL: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

2. Carnegie Mellon University, Software Engineering Institute. (2017). Defining the Relationships Between BCM, BCP, DRP, and COOP.

Page 2: "The BCP is the documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical products and services..." This source explicitly links the BCP to the continuity of critical services.

URL: https://resources.sei.cmu.edu/assetfiles/WhitePaper/2017019001503527.pdf

Question: 14

A company's user accounts have been compromised. Users are also reporting that the company's internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

A: There is an issue with the SSL certificate causing port 443 to become unavailable for HTTPS access

B: An on-path attack is being performed by someone with internal access that forces users into port 80

C: The web server cannot handle an increasing amount of HTTPS requests so it forwards users to port 80

D: An error was caused by BGP due to new rules applied over the company's internal routers

Correct Answer:

B

Explanation:

The symptoms described—compromised accounts and intermittent downgrading from HTTPS to HTTP—are classic indicators of an on-path attack (formerly Man-in-the-Middle). An attacker with a foothold on the internal network intercepts the user's initial connection request. The attacker then establishes an unencrypted HTTP (port 80) session with the user while maintaining the secure HTTPS session with the server. This technique, known as SSL stripping, allows the attacker to capture credentials and other sensitive data in cleartext, explaining the compromised accounts. The intermittent nature is consistent with an active attack rather than a static configuration error.

Why Incorrect Options are Wrong:

A: An SSL certificate issue would typically result in browser security warnings or connection failures, not a silent, intermittent downgrade to an unencrypted HTTP connection.

C: A web server handling high load would queue requests or return an error; it would not be configured to insecurely downgrade users to HTTP as a standard load-balancing measure.

D: BGP is an exterior gateway protocol used for routing between autonomous systems on the internet, not typically for an internal portal. A routing error would cause connectivity loss, not a protocol downgrade.

References:

1. CompTIA CySA+ CS0-003 Study Guide. (2023). Sybex, Wiley. Objective 1.2, "Given a scenario, analyze indicators of compromise." On-path attacks are a key topic where attackers intercept and often downgrade connections to capture data.

2. Seth, I., & Bissyandé, T. F. (2018). A study of the practicality of SSL/TLS interception attacks. IEEE. This paper discusses the mechanics of on-path attacks, including SSL stripping, where an attacker forces a victim's browser to use HTTP instead of HTTPS.

3. MIT OpenCourseWare. (2014). 6.857 Computer and Network Security, Fall 2014. Lecture 12: Web Security. Massachusetts Institute of Technology. The lecture materials describe how an active network attacker can perform an on-path attack to strip SSL/TLS protections from a user's session, downgrading it to plain HTTP.

Question: 15

Which of the following items should be included in a vulnerability scan report? (Choose two.)

A: Lessons learned

B: Service-level agreement

C: Playbook

D: Affected hosts

E: Risk score

F: Education plan

Correct Answer:

D, E

Explanation:

A vulnerability scan report is a technical document designed to communicate the findings of a security assessment. Its core purpose is to enable effective remediation. Therefore, it must include a list of the specific systems found to be vulnerable, which are the affected hosts. To prioritize remediation efforts, the report must also quantify the severity of each finding, typically through a risk score (e.g., CVSS - Common Vulnerability Scoring System). These two elements are fundamental to the report's utility in a vulnerability management program.

Why Incorrect Options are Wrong:

A: Lessons learned: This is a component of a post-incident review or after-action report, not a standard vulnerability scan report which focuses on technical findings.

B: Service-level agreement: An SLA is a contractual document defining service expectations; it is not part of the technical output of a vulnerability scan.

C: Playbook: A playbook contains standardized procedures for incident response; it is a response tool, not a report of discovered vulnerabilities.

F: Education plan: An education plan is a training initiative. While scan results might inform it, the plan itself is a separate document.

References:

1. National Institute of Standards and Technology (NIST). (2008). Special Publication 800-115, Technical Guide to Information Security Testing and Assessment. Section 6.2, "Reporting," states that a security assessment report should include "a listing of the systems that were found to have vulnerabilities" (Affected hosts) and "a rating for each vulnerability" (Risk score) to assist in prioritization. (p. 58). https://csrc.nist.gov/publications/detail/sp/800-115/final

2. CompTI(2023). CompTIA Cybersecurity Analyst (CySA+) CS0-003 Exam Objectives. Objective 1.2, "Given a scenario, perform vulnerability management," requires the analyst to "analyze the output from a vulnerability scanner," which inherently includes identifying affected systems and understanding severity/risk scores for prioritization. (p. 4). https://comptia.jp/pdf/CompTIA%20CySA+%20(CS0-003)%20Exam%20Objectives%20(3.0).pdf%20Exam%20Objectives%20(3.0).pdf)

Question: 16

Which of the following is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system?

A: Mean time to detect

B: Number of exploits by tactic

C: Alert volume

D: Quantity of intrusion attempts

Correct Answer:

A

Explanation:

The primary purpose of investing in a Security Information and Event Management (SIEM) system is to enhance an organization's ability to detect security incidents by correlating log data from multiple sources. Mean Time to Detect (MTTD) is a key performance indicator (KPI) that directly measures the average time it takes from when an incident occurs to when it is discovered by the security team. A lower MTTD indicates that the SIEM and associated processes are effective. The SOAR and ticketing systems then act on these detections, but the initial detection efficiency, measured by MTTD, is the foundational metric demonstrating the SIEM's value.

Why Incorrect Options are Wrong:

B: Number of exploits by tactic: This is a threat intelligence metric that describes adversary behavior; it does not measure the performance or efficiency of the organization's internal security tools.

C: Alert volume: This metric can be misleading. A high volume could indicate poor SIEM tuning (many false positives) rather than effective detection, making it an unreliable measure of success.

D: Quantity of intrusion attempts: This measures external threat activity against the perimeter. It reflects the threat environment, not how well the internal SIEM/SOAR systems perform in detecting and responding to threats.

References:

1. MITRE Corporation. (2022). 11 Strategies of a World-Class Cybersecurity Operations Center (2nd ed.). Page 29. This document identifies Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) as the most common and fundamental metrics for measuring the performance of a Cybersecurity Operations Center (SOC), which leverages tools like SIEM and SOAR.

2. NIST Special Publication 800-92. (2009). Guide to Computer Security Log Management. Section 4.4. This guide discusses the use of log management infrastructure (like a SIEM) for security auditing and response, stating a key goal is "providing a trail of activities" to support "incident handling." The speed of this process (MTTD) is a direct measure of its effectiveness.

3. CompTIA CySA+ CS0-003 Exam Objectives. (2023). Domain 5.2, "Explain the incident response process." The official objectives outline the incident response lifecycle, which begins with "Detection and Analysis." MTTD is the primary metric for evaluating the performance of this initial, critical phase.

Question: 17

Which of the following is the first step that should be performed when establishing a disaster recovery plan?

A: Agree on the goals and objectives of the plan

B: Determine the site to be used during a disaster

C: Demonstrate adherence to a standard disaster recovery process

D: Identify applications to be run during a disaster

Correct Answer:

A

Explanation:

The initial step in creating any strategic plan, including a disaster recovery plan (DRP), is to establish its foundational goals and objectives. This phase defines the scope, purpose, and high-level requirements for the entire DRP effort. All subsequent activities, such as conducting a business impact analysis (BIA) to identify critical applications and determining recovery site strategies, are guided by these established goals. Without clear objectives, the planning process lacks direction and cannot effectively prioritize resources or actions.

Why Incorrect Options are Wrong:

B: Determine the site to be used during a disaster: Site selection is a tactical decision made after recovery requirements (RTO/RPO) are defined, which themselves are derived from the plan's initial goals.

C: Demonstrate adherence to a standard disaster recovery process: This is a validation or audit activity that occurs after the plan has been developed, implemented, and tested, not at the beginning of its creation.

D: Identify applications to be run during a disaster: This is a key part of the Business Impact Analysis (BIA), which is a very early step but follows the initial establishment of the plan's overall goals and objectives.

References:

National Institute of Standards and Technology (NIST) Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. Section 3, "Contingency Planning Process," outlines the seven-step process. Step 1 is "Develop the contingency

planning policy statement," which "establishes the organizational guidance and identify the high-level goals and objectives for the IT contingency program." This precedes Step 2, the Business Impact Analysis (BIA), where critical systems and applications are identified. (URL: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final, Page 13, Section 3).

CompTIA CySA+ CS0-003 Certification Study Guide. The process of business continuity and disaster recovery planning is consistently framed as beginning with a policy and scope definition, which encompasses setting goals and objectives. This foundational step directs the subsequent BIA and strategy development.

Question: 18

A security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM. The analyst no longer had to jump between tools. Which of the following best describes what the security program did?

A: Data enrichment

B: Security control plane

C: Threat feed combination

D: Single pane of glass

Correct Answer:

D

Explanation:

The term "single pane of glass" describes a management console that consolidates data and controls from multiple, disparate security tools into a single, unified interface. The primary benefit, as described in the scenario, is the improvement of operational efficiency—in this case, Mean Time to Respond (MTTR)—by eliminating the need for analysts to switch between different systems. Integrating security controls into a SIEM to create a centralized view for the analyst is a classic example of implementing a single pane of glass architecture.

Why Incorrect Options are Wrong:

A: Data enrichment: This is the process of adding contextual information to raw data (e.g., adding reputation data to an IP address), not the consolidation of tool interfaces.

B: Security control plane: This is a broader architectural term for the infrastructure that manages and enforces security policies across systems, not the user-facing console itself.

C: Threat feed combination: This refers to the specific act of aggregating multiple threat intelligence sources, which is a data input, not the unified interface that displays it.

References:

Palo Alto Networks. (n.d.). Cybersecurity Glossary: Single Pane of Glass. "A single pane of glass is a single management console for a system or a set of systems. The single pane of glass displays all the information you need to monitor the system(s) on one screen."

Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-a-single-pane-of-glass

CompTI(2023). CompTIA CySA+ (CS0-003) Exam Objectives. Section 1.3, "Given a scenario, perform vulnerability management." This objective includes integrating systems and data, a primary goal of which is to create a unified view for efficient analysis, as embodied by the single pane of glass concept.

IBM. (2023). What is a SIEM?. "SIEMs also streamline incident response by integrating with other security tools... to create a 'single pane of glass' for security analysts." Retrieved from https://www.ibm.com/topics/siem

Question: 19

Which of the following tools would work best to prevent the exposure of PII outside of an organization?

A: PAM

B: IDS

C: PKI

D: DLP

Correct Answer:

D

Explanation:

Data Loss Prevention (DLP) is a suite of technologies and processes specifically designed to prevent the unauthorized disclosure or exfiltration of sensitive information, such as Personally Identifiable Information (PII). DLP systems enforce security policies by monitoring data in use (on endpoints), in motion (across the network), and at rest (in storage). They can identify PII based on predefined patterns or custom rules and automatically block, encrypt, or quarantine any attempts to move that data outside the organization's control, directly fulfilling the requirement of the question.

Why Incorrect Options are Wrong:

A: PAM (Privileged Access Management): Focuses on securing, managing, and monitoring privileged accounts and their access to critical systems, not on preventing the exfiltration of specific data content.

B: IDS (Intrusion Detection System): A passive monitoring tool that generates alerts upon detecting suspicious activity or policy violations. It detects potential threats but does not actively block data from leaving.

C: PKI (Public Key Infrastructure): A framework for managing digital certificates and public-key encryption. While it can encrypt PII to protect its confidentiality, it does not prevent the data's transmission.

References:

CompTI(2023). CompTIA CySA+ (CS0-003) Exam Objectives. Section 1.3. "Data loss prevention (DLP)" is listed as a key security solution for infrastructure management. [Direct URL: https://comptia.jp/pdf/comptia-cysa-exam-objectives-cs0-003.pdf]

Vaidya, J., et al. (2015). Data Leakage Prevention. In Foundations and Trends® in Privacy and Security. Now Foundations and Trends. This academic publication defines DLP as a system to "prevent leakage of sensitive data from a system." (Page 1). [Direct URL: https://www.nowpublishers.com/article/Details/PGL-001]

Kent, S., & Souppaya, M. (2006). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. This document defines an IDS as a system that "monitors for suspicious activity... and produces reports," highlighting its detection-focused role. (Section 2.1, Page 2-1). [Direct URL: https://csrc.nist.gov/publications/detail/sp/800-94/final]

Question: 20

The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

A: Deploy a CASB and enable policy enforcement

B: Configure MFA with strict access

C: Deploy an API gateway

D: Enable SSO to the cloud applications

Correct Answer:

A

Explanation:

A Cloud Access Security Broker (CASB) is a security policy enforcement point placed between cloud service consumers and providers. Its primary functions include providing visibility into cloud service usage, a task known as discovery. This discovery function is crucial for identifying shadow IT—unapproved applications used by employees. Once discovered, a CASB can assess the risk of these applications and enforce granular security policies, such as blocking access to high-risk services, enforcing data loss prevention (DLP), and monitoring user activity. This directly addresses the CISO's goal of eliminating and reducing the risk posed by unsanctioned, high-risk cloud applications.

Why Incorrect Options are Wrong:

B: Multi-Factor Authentication (MFA) enhances security for known, sanctioned applications but cannot be applied to shadow IT services that the organization is unaware of.

C: An API gateway is used to secure and manage APIs that an organization exposes for its own services, not to monitor or control employee use of third-party cloud applications.

D: Single Sign-On (SSO) centralizes and simplifies user authentication for approved applications but does not provide the discovery or policy enforcement capabilities needed to manage shadow IT.

References:

1. National Institute of Standards and Technology (NIST). (2020). Special Publication 800-207: Zero Trust Architecture. Page 16, Section 3.2.2. This document describes how a Policy

Enforcement Point (PEP), such as a CASB, can "terminate a connection, session, or data packet and generate a log entry" for enterprise resources, which is fundamental to controlling access to unsanctioned cloud applications.

URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

2. Srinivas, J., Das, K., & Kumar, N. (2019). CASB: A Centralized Security Solution for Cloud Computing. 2019 International Conference on Communication and Signal Processing (ICCSP). IEEE. Page 0511. The paper states, "CASB helps in discovering the shadow IT and provides visibility and control over the cloud services." This directly supports the use of a CASB to identify and manage shadow IT.

URL: https://ieeexplore.ieee.org/document/8698001

3. CompTI(2023). CompTIA Cybersecurity Analyst (CySA+) CS0-003 Exam Objectives. Page 5, Domain 1.0, Objective 1.3. The official exam objectives list "CASB (Cloud access security broker)" as a key security solution for infrastructure management, confirming its relevance and importance within the CySA+ curriculum for securing cloud environments.

URL: https://comptia.jp/pdf/CompTIA%20CySA+%20(CS0-003)%20Exam%20Objectives%20(3.0).pdf%20Exam%20Objectives%20(3.0).pdf)

Question: 21

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

A: Hard disk

B: Primary boot partition

C: Malicious files

D: Routing table

E: Static IP address

Correct Answer:

D

Explanation:

The question requires identifying the most volatile piece of evidence to collect first, following the forensic principle of the order of volatility. The routing table is stored in the server's volatile memory (RAM) and contains dynamic information about network connections. This data will be lost or altered if the server is disconnected from the network (isolated) or powered down. Therefore, it must be collected before any other action is taken. Data on the hard disk, including partitions and files, is non-volatile and will persist through isolation or a reboot, allowing for later collection.

Why Incorrect Options are Wrong:

A: Hard disk: This is non-volatile storage. Its contents are preserved after power loss and should be imaged after collecting volatile data.

B: Primary boot partition: This is a section of the non-volatile hard disk and is collected during the disk imaging phase.

C: Malicious files: These files are located on the non-volatile hard disk and are preserved for later collection and analysis.

E: Static IP address: This is a configuration setting stored in a file on the hard disk, making it non-volatile.

References:

1. National Institute of Standards and Technology (NIST) Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response. Section 3.1.1, "Collecting Evidence," presents a table detailing the order of volatility. It lists "Routing tables, ARP cache, process tables, kernel statistics" as highly volatile data that should be collected before less volatile data like "Data on hard disk."

URL: https://csrc.nist.gov/publications/detail/sp/800-86/final (See Table 3-1 on page 17)

2. Internet Engineering Task Force (IETF) RFC 3227, Guidelines for Evidence Collection and Archiving. Section 3.2, "Order of Volatility," specifies that network information such as routing and ARP tables should be collected from a live system before non-volatile storage like disks.

URL: https://www.rfc-editor.org/rfc/rfc3227.html#section-3.2

3. Carnegie Mellon University, Software Engineering Institute, Best Practices in Digital Evidence Collection. This document reinforces the principle, stating, "The first rule of digital evidence collection is to collect the evidence in the order of its volatility... For example, the contents of system memory are more volatile than the contents of a hard drive."

URL: https://resources.sei.cmu.edu/assetfiles/WhitePaper/200201900152695.pdf (See page 4)

Question: 22

Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

A: Develop a call tree to inform impacted users

B: Schedule a review with all teams to discuss what occurred

C: Create an executive summary to update company leadership

D: Review regulatory compliance with public relations for official notification

Correct Answer:

B

Explanation:

The question asks for the best action to improve future incident response after an incident's conclusion. This directly corresponds to the "Post-Incident Activity" or "Lessons Learned" phase of the incident response lifecycle. Scheduling a review with all involved teams is the core of this phase. This meeting's purpose is to analyze the entire response process—what succeeded, what failed, and what could be done better—to generate actionable improvements. This is the most fundamental step toward enhancing future incident response capabilities.

Why Incorrect Options are Wrong:

A: Develop a call tree to inform impacted users: This is a specific preparatory task. The need for it would be identified during the lessons-learned review, making it a result of the review, not the review itself.

C: Create an executive summary to update company leadership: This is a reporting function focused on communicating the impact of the past incident to stakeholders, not the primary mechanism for process improvement for future incidents.

D: Review regulatory compliance with public relations for official notification: This is a specific compliance and external communication task, not the comprehensive internal review aimed at improving the overall incident response process and security posture.

References:

NIST Special Publication 800-61 Rev. 2, "Computer Security Incident Handling Guide": Section 3.4, "Post-Incident Activity" (page 29), explicitly states, "Holding a 'lessons learned'

meeting with all involved parties after a major incident is a major component of this phase... The meeting provides a chance to achieve closure... by reviewing what occurred, what was done to intervene, and how well intervention worked." This directly supports the action of scheduling a review.

URL: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Carnegie Mellon University, Software Engineering Institute (SEI), "Defining the 'Postmortem' Process for Incident Response": Section 2, "The Postmortem Process" (page 2), describes the postmortem as a structured review meeting held after an incident. Its goals are to understand the timeline, analyze the response, and identify follow-up actions to improve future performance, which aligns perfectly with the correct answer.

URL: https://resources.sei.cmu.edu/assetfiles/WhitePaper/2016019001453721.pdf

Question: 23

An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

A: Beaconing

B: Domain Name System hijacking

C: Social engineering attack

D: On-path attack

E: Obfuscated links

F: Address Resolution Protocol poisoning

Correct Answer:

C, E

Explanation:

The scenario describes a targeted email campaign against company administrators, which is a form of social engineering attack. Specifically, it aligns with spear phishing, where attackers craft messages for specific, high-value individuals or groups. The use of a "concealed URL" is a direct implementation of obfuscated links. Attackers use obfuscation techniques (e.g., URL shortening, character encoding) to hide the true, malicious destination of the link from both the user and security filters, thereby increasing the likelihood of a successful compromise.

Why Incorrect Options are Wrong:

A: Beaconing: This is post-compromise communication where malware periodically contacts a command-and-control server. The scenario describes the initial attack delivery, not subsequent malware activity.

B: Domain Name System hijacking: This attack redirects legitimate DNS queries to malicious servers. The scenario does not provide evidence that DNS resolution itself has been compromised.

D: On-path attack: This involves an attacker intercepting and potentially altering communications between two parties. The scenario describes a direct communication (email) to the target, not an interception.

F: Address Resolution Protocol poisoning: This is a Layer 2 attack on a local area network to intercept traffic by falsifying MAC-to-IP address mappings, which is irrelevant to an email-based attack.

References:

1. Social Engineering: CompTI(2023). CompTIA CySA+ (CS0-003) Certification Study Guide. "Social engineering is an attack that targets the human element of security... Spear phishing is a targeted form of phishing where the attacker has some information about the target." (Domain 1: Security Operations, Objective 1.1).

2. Obfuscation: McMillan, T. (2023). CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-003). McGraw-Hill. In discussions of malware and attack techniques, obfuscation is defined as the practice of making code or data difficult for humans and security tools to understand. Concealing a URL's true destination is a primary example of this. (Chapter 3: Analyzing the Threat Landscape).

3. Attack Vector Analysis: National Institute of Standards and Technology (NIST). (2012). SP 800-61 Rev. 2, Computer Security Incident Handling Guide. Section 2.3.1 describes attack vectors, including social engineering (e.g., phishing emails) used to trick users into clicking malicious links or opening attachments. Page 11. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Question: 24

A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

A: Testing

B: Implementation

C: Validation

D: Rollback

Correct Answer:

C

Explanation:

The vulnerability management lifecycle is a structured process. The question describes the completion of the implementation phase, where a patch is "applied." According to standard cybersecurity procedures, the immediate next step is to validate that the remediation action was successful. Validation involves verifying that the patch has effectively closed the specific vulnerability it was intended to address and has not introduced new security flaws. This is typically accomplished by re-scanning the system or performing a targeted security check to confirm the vulnerability is no longer detectable.

Why Incorrect Options are Wrong:

A: Testing: While validation is a form of testing, "validation" is the more precise term for the post-remediation activity of confirming a fix. General testing often occurs before deploying a patch in production.

B: Implementation: The question states the patch has already been "applied," which constitutes the implementation step. Therefore, it cannot be the next step.

D: Rollback: A rollback is a contingency plan executed only if the validation step fails or the patch causes critical operational issues. It is not the standard subsequent step.

References:

NIST Special Publication 800-40 Revision 3, Guide to Enterprise Patch Management Technologies: Section 2.2, "Patch Management Process," outlines the key phases. After "Patch Installation" (Implementation), the next phase is "Patch Compliance Verification" (Validation), which "involves verifying that patches have been installed correctly." (Page 10).

URL: https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final

CompTIA CySA+ CS0-003 Exam Objectives: Domain 1.0, "Security Operations," objective 1.3, "Given a scenario, apply the appropriate vulnerability management techniques," implicitly covers this lifecycle. The logical flow is identification, analysis, remediation (implementation), and then validation/verification of the fix.

URL: https://comptia.jp/pdf/comptia-cysa-cs0-003-exam-objectives-3-0.pdf (Page 6)

Carnegie Mellon University, CERT Coordination Center (CERT/CC): The CERT/CC vulnerability response process includes a "Remediation" phase. This phase consists of applying the fix and then verifying that the fix is effective, which aligns directly with the concept of post-implementation validation.

URL: https://insights.sei.cmu.edu/blog/a-coordination-centric-view-of-vulnerability-management/

Question: 25

A company is implementing a vulnerability management program and moving from an on-premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?

A: The current scanners should be migrated to the cloud

B: Cloud-specific misconfigurations may not be detected by the current scanners

C: Existing vulnerability scanners cannot scan IaaS systems

D: Vulnerability scans on cloud environments should be performed from the cloud

Correct Answer:

B

Explanation:

When an organization transitions to a hybrid IaaS model, it introduces a new layer of potential security weaknesses: cloud service configurations. Traditional vulnerability scanners are primarily designed to detect software vulnerabilities (e.g., CVEs) within operating systems and applications. However, they often lack the capability to analyze cloud-specific settings such as Identity and Access Management (IAM) role permissions, security group rules, or storage bucket policies. These misconfigurations are a leading cause of cloud security breaches. Therefore, a critical implication for the vulnerability management program is recognizing that existing tools may have a significant visibility gap in the new cloud environment.

Why Incorrect Options are Wrong:

A: Migrating scanners is an architectural decision for performance or cost, not a fundamental implication. Scanners can operate effectively from on-premises if configured correctly.

C: This statement is factually incorrect. Standard vulnerability scanners can and do scan IaaS instances (virtual machines), as they function like traditional servers.

D: While scanning from within the cloud is often a best practice to reduce latency and data transfer costs, it is not a mandatory requirement or the core issue.

References:

1. CompTIA CySA+ CS0-003 Certification Study Guide: In discussing cloud security, the guide emphasizes the shared responsibility model and the new types of vulnerabilities introduced by cloud platforms. It notes, "Misconfigurations of cloud environments are a common source of security vulnerabilities... Tools like cloud security posture management (CSPM) solutions are designed to detect these misconfigurations." This supports the idea that traditional scanners (option B) may not be sufficient. (Chapple, M., & Seidl, (2023). CompTIA CySA+ Study Guide: Exam CS0-003. John Wiley & Sons. Domain 1, Objective 1.3).

2. NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing: This document outlines security considerations for cloud computing. It highlights that "the external-facing management API for the cloud... is a major new potential vector of attack." This management plane is where misconfigurations occur, an area traditional scanners may not cover. (NIST SP 800-144, Section 5.2.2, Page 18).

3. IEEE Publication on Cloud Security: Research in cloud security consistently differentiates between vulnerabilities within a virtual machine and misconfigurations of the cloud infrastructure itself. A paper states, "While traditional security solutions can be deployed to protect the guest OS and applications, securing the cloud infrastructure control plane requires specialized approaches." This confirms that existing scanners may not detect cloud-specific issues. (Habib, S. M., et al. (2015). "A Security Architecture for Cloud-Centric IoT." IEEE Cloud Computing).

Question: 26

An organization has experienced a breach of customer transactions. Under the terms of PCI DSS, which of the following groups should the organization report the breach to?

A: PCI Security Standards Council

B: Local law enforcement

C: Federal law enforcement

D: Card issuer

Correct Answer:

D

Explanation:

Under the Payment Card Industry Data Security Standard (PCI DSS), if an organization experiences a data breach involving cardholder data, it is required to report the incident to its acquirer (merchant bank) and the relevant payment card brands (e.g., Visa, Mastercard). This established reporting chain ensures that the card issuers (the banks that provide payment cards to consumers) are promptly notified. The issuers are critical in the response process as they are responsible for monitoring compromised accounts for fraud, notifying cardholders, and reissuing cards to prevent further financial harm.

Why Incorrect Options are Wrong:

A: PCI Security Standards Council: The PCI SSC is a global body that develops and maintains the PCI standards; it does not handle breach reporting, investigations, or enforcement.

B: Local law enforcement: While reporting to law enforcement is often a best practice and may be required by regional laws, it is not a specific reporting requirement mandated by the PCI DSS itself.

C: Federal law enforcement: Similar to local law enforcement, reporting to federal agencies is not a direct requirement of the PCI DSS, although it may be necessary under other legal or regulatory frameworks.

References:

PCI Security Standards Council, "Responding to a Data Breach: A Merchant's Guide": This official guide outlines the immediate response steps. Step 1 is "Immediately contact your

acquirer (merchant bank) and payment card brand(s)." The guide clarifies this process is to ensure all affected parties, including issuers, are notified. (Source: PCI Security Standards Council, Document Library).

Visa Inc., "What To Do If Compromised": Visa's official procedure for merchants states, "Alert all relevant parties. Your acquirer must notify Visa and other payment card brands of the suspected or confirmed compromise." This process directly leads to the notification of card issuers to protect cardholder accounts. (Page 3).

NIST Special Publication 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)": While not a PCI document, this publication discusses breach response and notes that industry-specific regulations like PCI DSS have their own reporting requirements to entities within that industry's ecosystem, such as card issuers and brands, distinct from general legal reporting. (Section 5.2).

Question: 27

The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released. Which of the following would best protect this organization?

A: A mean time to remediate of 30 days

B: A mean time to detect of 45 days

C: A mean time to respond of 15 days

D: Third-party application testing

Correct Answer:

A

Explanation:

The scenario presents a specific threat intelligence data point: attackers are exploiting vulnerabilities approximately 45 days after a patch is released. The most effective protection is to close this window of opportunity by fixing the vulnerability before it can be exploited. A Mean Time to Remediate (MTTR) of 30 days means the organization, on average, applies the necessary patches and fixes the vulnerability within 30 days. This ensures the system is secured well before the 45-day exploitation timeline, directly mitigating the specified risk. This is a proactive and preventative control that addresses the core problem.

Why Incorrect Options are Wrong:

B: A mean time to detect of 45 days: This is a reactive metric measuring the time to discover an attack after it has already occurred. It offers no proactive protection against the initial exploitation.

C: A mean time to respond of 15 days: This is also a reactive metric, measuring the time to contain and eradicate a threat after it has been detected. It does not prevent the initial compromise.

D: Third-party application testing: This is a process for discovering unknown vulnerabilities. The scenario concerns known vulnerabilities for which a patch is already available, making patch management the relevant control.

References:

1. CompTIA CySA+ CS0-003 Certification Study Guide, 3rd Edition. (Sybex, 2023). Chapter 3, "Analyzing Vulnerability Scans," discusses vulnerability management metrics. It defines Mean Time to Remediate (MTTR) as the average time it takes to fix a vulnerability after discovery, emphasizing that a lower MTTR is crucial for reducing the attack surface before exploitation can occur.

2. National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. The RA-5 (Vulnerability Monitoring and Scanning) control family emphasizes the importance of remediating vulnerabilities within organizationally-defined time frames based on risk. The scenario provides the risk (exploitation at 45 days), and an MTTR of 30 days is the appropriate time frame.

3. Kim, D., & Solomon, M. G. (2021). Fundamentals of Information Systems Security. Jones & Bartlett Learning. Chapter 11, "Security Operations," explains that effective vulnerability management programs prioritize patching based on threat intelligence, aiming to remediate vulnerabilities before they are widely exploited, which directly aligns with the logic of selecting an MTTR of 30 days.

Question: 28

An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

A: Exploitation

B: Reconnaissance

C: Command and control

D: Actions on objectives

Correct Answer:

B

Explanation:

The activity described, where an external IP address conducts network and vulnerability scans, is a definitive example of the Reconnaissance phase of an attack framework. During this initial stage, an adversary actively probes a target's perimeter to gather information, identify open ports, discover running services, and find potential vulnerabilities. This information is then used to plan subsequent stages of the attack, such as exploitation.

Why Incorrect Options are Wrong:

A: Exploitation: This phase involves actively using a discovered vulnerability to gain unauthorized access, which is a step that would follow the described scanning activity.

C: Command and control: This occurs after a system has been successfully compromised, establishing a communication channel for the attacker to issue commands to the infected host.

D: Actions on objectives: This is the final phase where the attacker carries out their ultimate goal (e.g., data exfiltration), which happens much later in the attack lifecycle.

References:

1. MITRE ATT&CK® Framework. The "Reconnaissance" tactic (TA0043) is defined as gathering information to plan future adversary operations. The technique "Active Scanning" (T1595) specifically describes this activity: "Adversaries may execute active scans of victim hosts to gather information."

Source: MITRE. (2024). Reconnaissance, Tactic TA0043. MITRE ATT&CK. Retrieved from https://attack.mitre.org/tactics/TA0043/

Source: MITRE. (2024). Active Scanning, Technique T1595. MITRE ATT&CK. Retrieved from https://attack.mitre.org/techniques/T1595/

2. National Institute of Standards and Technology (NIST). NIST Special Publication 800-115 describes the phases of security testing, where the initial phase involves information gathering and discovery (reconnaissance) through techniques like network and vulnerability scanning.

Source: Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, (2008). Technical Guide to Information Security Testing and Assessment (NIST SP 800-115). Section 3.2, "Discovery." Retrieved from https://csrc.nist.gov/publications/detail/sp/800-115/final