

Exam : SY0-701

Title : CompTIA Security+

Version : V12.02

1. Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?

- A. Hacktivist
- B. Whistleblower
- C. Organized crime
- D. Unskilled attacker

Answer: C

Explanation:

Organized crime is a type of threat actor that is motivated by financial gain and often operates across national borders. Organized crime groups may be hired by foreign governments to conduct cyberattacks on critical systems located in other countries, such as power grids, military networks, or financial institutions. Organized crime groups have the resources, skills, and connections to carry out sophisticated and persistent attacks that can cause significant damage and disruption¹².

Reference = 1: Threat Actors - CompTIA Security+ SY0-701 - 2.1 2: CompTIA Security+ SY0-701 Certification Study Guide

2. Which of the following is used to add extra complexity before using a one-way data transformation algorithm?

- A. Key stretching
- B. Data masking
- C. Steganography
- D. Salting

Answer: D

Explanation:

Salting is the process of adding extra random data to a password or other data before applying a one-way data transformation algorithm, such as a hash function. Salting increases the complexity and randomness of the input data, making it harder for attackers to guess or crack the original data using precomputed tables or brute force methods. Salting also helps prevent identical passwords from producing identical hash values, which could reveal the passwords to attackers who have access to the hashed data. Salting is commonly used to protect passwords stored in databases or transmitted over networks.

Reference =

Passwords technical overview

Encryption, hashing, salting – what's the difference?

Salt (cryptography)

3. An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a “page not found” error message.

Which of the following types of social engineering attacks occurred?

- A. Brand impersonation
- B. Pretexting
- C. Typosquatting

D. Phishing

Answer: D

Explanation:

Phishing is a type of social engineering attack that involves sending fraudulent emails that appear to be from legitimate sources, such as payment websites, banks, or other trusted entities. The goal of phishing is to trick the recipients into clicking on malicious links, opening malicious attachments, or providing sensitive information, such as log-in credentials, personal data, or financial details. In this scenario, the employee received an email from a payment website that asked the employee to update contact information. The email contained a link that directed the employee to a fake website that mimicked the appearance of the real one. The employee entered the log-in information, but received a “page not found” error message. This indicates that the employee fell victim to a phishing attack, and the attacker may have captured the employee’s credentials for the payment website.

Reference = Other Social Engineering Attacks – CompTIA Security+ SY0-701 – 2.2, CompTIA Security+: Social Engineering Techniques & Other Attack ... - NICCS, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

4. An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25.

Which of the following firewall ACLs will accomplish this goal?

A. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 10.50.10.25 32 0.0.0.0/0 port 53

B. Access list outbound permit 0.0.0.0/0 10.50.10.25 32 port 53 Access list outbound deny 0.0.0.0 0 0.0.0.0/0 port 53

C. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 10.50.10.25 32 port 53

D. Access list outbound permit 10.50.10.25 32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0.0.0.0.0/0 port 53

Answer: D

Explanation:

The correct answer is D because it allows only the device with the IP address 10.50.10.25 to send outbound DNS requests on port 53, and denies all other devices from doing so. The other options are incorrect because they either allow all devices to send outbound DNS requests (A and C), or they allow no devices to send outbound DNS requests (B).

Reference = You can learn more about firewall ACLs and DNS in the following resources:

CompTIA Security+ SY0-701 Certification Study Guide, Chapter 4: Network Security¹

Professor Messer’s CompTIA SY0-701 Security+ Training Course, Section 3.2: Firewall Rules²

TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 6: Network Security, Lecture 28: Firewall Rules³

5. A data administrator is configuring authentication for a SaaS application and would like to reduce the number of credentials employees need to maintain. The company prefers to use domain credentials to access new SaaS applications.

Which of the following methods would allow this functionality?

A. SSO

- B. LEAP
- C. MFA
- D. PEAP

Answer: A

Explanation:

SSO stands for single sign-on, which is a method of authentication that allows users to access multiple applications or services with one set of credentials. SSO reduces the number of credentials employees need to maintain and simplifies the login process. SSO can also improve security by reducing the risk of password reuse, phishing, and credential theft. SSO can be implemented using various protocols, such as SAML, OAuth, OpenID Connect, and Kerberos, that enable the exchange of authentication information between different domains or systems. SSO is commonly used for accessing SaaS applications, such as Office 365, Google Workspace, Salesforce, and others, using domain credentials¹²³.

B. LEAP stands for Lightweight Extensible Authentication Protocol, which is a Cisco proprietary protocol that provides authentication for wireless networks. LEAP is not related to SaaS applications or domain credentials⁴.

C. MFA stands for multi-factor authentication, which is a method of authentication that requires users to provide two or more pieces of evidence to prove their identity. MFA can enhance security by adding an extra layer of protection beyond passwords, such as tokens, biometrics, or codes. MFA is not related to SaaS applications or domain credentials, but it can be used in conjunction with SSO.

D. PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that provides secure authentication for wireless networks. PEAP uses TLS to create an encrypted tunnel between the client and the server, and then uses another authentication method, such as MS-CHAPv2 or EAP-GTC, to verify the user's identity. PEAP is not related to SaaS applications or domain credentials.

Reference = 1: Security+ (SY0-701) Certification Study Guide | CompTIA IT Certifications 2: What is Single Sign-On (SSO)? - Definition from WhatIs.com 3: Single sign-on - Wikipedia 4: Lightweight Extensible Authentication Protocol - Wikipedia: What is Multi-Factor Authentication (MFA)? - Definition from WhatIs.com: Protected Extensible Authentication Protocol - Wikipedia

6. Which of the following scenarios describes a possible business email compromise attack?

- A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.
- B. Employees who open an email attachment receive messages demanding payment in order to access files.
- C. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
- D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

Answer: A

Explanation:

A business email compromise (BEC) attack is a type of phishing attack that targets employees who have access to company funds or sensitive information. The attacker impersonates a trusted person, such as an executive, a vendor, or a client, and requests a fraudulent payment, a wire transfer, or confidential data. The attacker often uses social engineering techniques, such as urgency, pressure, or familiarity, to

convince the victim to comply with the request¹².

In this scenario, option A describes a possible BEC attack, where an employee receives a gift card request in an email that has an executive's name in the display field of the email. The email may look like it is coming from the executive, but the actual email address may be spoofed or compromised. The attacker may claim that the gift cards are needed for a business purpose, such as rewarding employees or clients, and ask the employee to purchase them and send the codes. This is a common tactic used by BEC attackers to steal money from unsuspecting victims³⁴.

Option B describes a possible ransomware attack, where malicious software encrypts the files on a device and demands a ransom for the decryption key. Option C describes a possible credential harvesting attack, where an attacker tries to obtain the login information of a privileged account by posing as a legitimate authority. Option D describes a possible phishing attack, where an attacker tries to lure the victim to a fake website that mimics the company's email portal and capture their credentials.

These are all types of cyberattacks, but they are not examples of BEC attacks.

Reference =

- 1: Business Email Compromise - CompTIA Security+ SY0-701 - 2.2
- 2: CompTIA Security+ SY0-701 Certification Study Guide
- 3: Business Email Compromise: The 12 Billion Dollar Scam
- 4: TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy

7. A company prevented direct access from the database administrators' workstations to the network segment that contains database servers.

Which of the following should a database administrator use to access the database servers?

- A. Jump server
- B. RADIUS
- C. HSM
- D. Load balancer

Answer: A

Explanation:

A jump server is a device or virtual machine that acts as an intermediary between a user's workstation and a remote network segment. A jump server can be used to securely access servers or devices that are not directly reachable from the user's workstation, such as database servers. A jump server can also provide audit logs and access control for the remote connections. A jump server is also known as a jump box or a jump host¹².

RADIUS is a protocol for authentication, authorization, and accounting of network access. RADIUS is not a device or a method to access remote servers, but rather a way to verify the identity and permissions of users or devices that request network access³⁴.

HSM is an acronym for Hardware Security Module, which is a physical device that provides secure storage and generation of cryptographic keys. HSMs are used to protect sensitive data and applications, such as digital signatures, encryption, and authentication. HSMs are not used to access remote servers, but rather to enhance the security of the data and applications that reside on them⁵.

A load balancer is a device or software that distributes network traffic across multiple servers or devices, based on criteria such as availability, performance, or capacity. A load balancer can improve the scalability, reliability, and efficiency of network services, such as web servers, application servers, or

database servers. A load balancer is not used to access remote servers, but rather to optimize the delivery of the services that run on them.

Reference =

How to access a remote server using a jump host

Jump server

RADIUS

Remote Authentication Dial-In User Service (RADIUS)

Hardware Security Module (HSM)

[What is an HSM?]

[Load balancing (computing)]

[What is Load Balancing?]

8. An organization's internet-facing website was compromised when an attacker exploited a buffer overflow.

Which of the following should the organization deploy to best protect against similar attacks in the future?

A. NGFW

B. WAF

C. TLS

D. SD-WAN

Answer: B

Explanation:

A buffer overflow is a type of software vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. This can lead to unexpected behavior, such as crashes, errors, or code execution. A buffer overflow can be exploited by an attacker to inject malicious code or commands into the application, which can compromise the security and functionality of the system. An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. To best protect against similar attacks in the future, the organization should deploy a web application firewall (WAF). A WAF is a type of firewall that monitors and filters the traffic between a web application and the internet. A WAF can detect and block common web attacks, such as buffer overflows, SQL injections, cross-site scripting (XSS), and more. A WAF can also enforce security policies and rules, such as input validation, output encoding, and encryption. A WAF can provide a layer of protection for the web application, preventing attackers from exploiting its vulnerabilities and compromising its data.

Reference = Buffer Overflows – CompTIA Security+ SY0-701 – 2.3, Web Application Firewalls – CompTIA Security+ SY0-701 – 2.4, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

9. An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords.

Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

A. Multifactor authentication

- B. Permissions assignment
- C. Access management
- D. Password complexity

Answer: A

Explanation:

The correct answer is A because multifactor authentication (MFA) is a method of verifying a user's identity by requiring more than one factor, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access even if the user's password is compromised, as the attacker would need to provide another factor to log in. The other options are incorrect because they do not address the root cause of the attack, which is weak authentication. Permissions assignment (B) is the process of granting or denying access to resources based on the user's role or identity. Access management © is the process of controlling who can access what and under what conditions. Password complexity (D) is the requirement of using strong passwords that are hard to guess or crack, but it does not prevent an attacker from using a stolen password.

Reference = You can learn more about multifactor authentication and other security concepts in the following resources:

CompTIA Security+ SY0-701 Certification Study Guide, Chapter 1: General Security Concepts¹

Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.2: Security Concepts²

Multi-factor Authentication – SY0-601 CompTIA Security+: 2.43

TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 3: Identity and Access Management, Lecture 15: Multifactor Authentication⁴

CompTIA Security+ Certification SY0-601: The Total Course [Video], Chapter 3: Identity and Account Management, Section 2: Enabling Multifactor Authentication⁵

10. An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification.

Which of the following social engineering techniques are being attempted? (Choose two.)

- A. Typosquatting
- B. Phishing
- C. Impersonation
- D. Vishing
- E. Smishing
- F. Misinformation

Answer: B E

Explanation:

Smishing is a type of social engineering technique that uses text messages (SMS) to trick victims into revealing sensitive information, clicking malicious links, or downloading malware. Smishing messages often appear to come from legitimate sources, such as banks, government agencies, or service providers, and use urgent or threatening language to persuade the recipients to take action¹². In this scenario, the text message that claims to be from the payroll department is an example of smishing. Impersonation is a type of social engineering technique that involves pretending to be someone else, such as an authority figure, a trusted person, or a colleague, to gain the trust or cooperation of the target. Impersonation can be done through various channels, such as phone calls, emails, text messages, or in-

person visits, and can be used to obtain information, access, or money from the victim³⁴. In this scenario, the text message that pretends to be from the payroll department is an example of impersonation.

A. Typosquatting is a type of cyberattack that involves registering domain names that are similar to popular or well-known websites, but with intentional spelling errors or different extensions. Typosquatting aims to exploit the common mistakes that users make when typing web addresses, and redirect them to malicious or fraudulent sites that may steal their information, install malware, or display ads⁵⁶. Typosquatting is not related to text messages or credential verification.

B. Phishing is a type of social engineering technique that uses fraudulent emails to trick recipients into revealing sensitive information, clicking malicious links, or downloading malware. Phishing emails often mimic the appearance and tone of legitimate organizations, such as banks, retailers, or service providers, and use deceptive or urgent language to persuade the recipients to take action⁷⁸. Phishing is not related to text messages or credential verification.

D. Vishing is a type of social engineering technique that uses voice calls to trick victims into revealing sensitive information, such as passwords, credit card numbers, or bank account details. Vishing calls often appear to come from legitimate sources, such as law enforcement, government agencies, or technical support, and use scare tactics or false promises to persuade the recipients to comply⁹. Vishing is not related to text messages or credential verification.

F. Misinformation is a type of social engineering technique that involves spreading false or misleading information to influence the beliefs, opinions, or actions of the target. Misinformation can be used to manipulate public perception, create confusion, damage reputation, or promote an agenda. Misinformation is not related to text messages or credential verification.

Reference = 1: What is Smishing? | Definition and Examples | Kaspersky 2: Smishing - Wikipedia 3: Impersonation Attacks: What Are They and How Do You Protect Against Them? 4: Impersonation - Wikipedia 5: What is Typosquatting? | Definition and Examples | Kaspersky 6: Typosquatting - Wikipedia 7: What is Phishing? | Definition and Examples | Kaspersky 8: Phishing - Wikipedia 9: What is Vishing? | Definition and Examples | Kaspersky: Vishing - Wikipedia: What is Misinformation? | Definition and Examples | Britannica: Misinformation - Wikipedia

11. Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO).

The message stated: "I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address."

Which of the following are the best responses to this situation? (Choose two).

- A. Cancel current employee recognition gift cards.
- B. Add a smishing exercise to the annual company training.
- C. Issue a general email warning to the company.
- D. Have the CEO change phone numbers.
- E. Conduct a forensic investigation on the CEO's phone.
- F. Implement mobile device management.

Answer: B, C

Explanation:

This situation is an example of smishing, which is a type of phishing that uses text messages (SMS) to entice individuals into providing personal or sensitive information to cybercriminals. The best responses

to this situation are to add a smishing exercise to the annual company training and to issue a general email warning to the company. A smishing exercise can help raise awareness and educate employees on how to recognize and avoid smishing attacks. An email warning can alert employees to the fraudulent text message and remind them to verify the identity and legitimacy of any requests for information or money.

Reference = What Is Phishing | Cybersecurity | CompTIA, Phishing – SY0-601 CompTIA Security+: 1.1 - Professor Messer IT Certification Training Courses

12. A company is required to use certified hardware when building networks.

Which of the following best addresses the risks associated with procuring counterfeit hardware?

- A. A thorough analysis of the supply chain
- B. A legally enforceable corporate acquisition policy
- C. A right to audit clause in vendor contracts and SOWs
- D. An in-depth penetration test of all suppliers and vendors

Answer: A

Explanation:

Counterfeit hardware is hardware that is built or modified without the authorization of the original equipment manufacturer (OEM). It can pose serious risks to network quality, performance, safety, and reliability¹². Counterfeit hardware can also contain malicious components that can compromise the security of the network and the data that flows through it³. To address the risks associated with procuring counterfeit hardware, a company should conduct a thorough analysis of the supply chain, which is the network of entities involved in the production, distribution, and delivery of the hardware. By analyzing the supply chain, the company can verify the origin, authenticity, and integrity of the hardware, and identify any potential sources of counterfeit or tampered products.

A thorough analysis of the supply chain can include the following steps:

Establishing a trusted relationship with the OEM and authorized resellers

Requesting documentation and certification of the hardware from the OEM or authorized resellers

Inspecting the hardware for any signs of tampering, such as mismatched labels, serial numbers, or components

Testing the hardware for functionality, performance, and security

Implementing a tracking system to monitor the hardware throughout its lifecycle

Reporting any suspicious or counterfeit hardware to the OEM and law enforcement agencies

Reference = 1: Identify Counterfeit and Pirated Products - Cisco, 2: What Is Hardware Security?

Definition, Threats, and Best Practices, 3: Beware of Counterfeit Network Equipment - TechNewsWorld,:

Counterfeit Hardware: The Threat and How to Avoid It

13. Which of the following provides the details about the terms of a test with a third-party penetration tester?

- A. Rules of engagement
- B. Supply chain analysis
- C. Right to audit clause
- D. Due diligence

Answer: A

Explanation:

Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable. Rules of engagement typically include the following elements:

The type and scope of the test, such as black box, white box, or gray box, and the target systems, networks, applications, or data.

The client contact details and the communication channels for reporting issues, incidents, or emergencies during the test.

The testing team credentials and the authorized tools and techniques that they can use.

The sensitive data handling and encryption requirements, such as how to store, transmit, or dispose of any data obtained during the test.

The status meeting and report schedules, formats, and recipients, as well as the confidentiality and non-disclosure agreements for the test results.

The timeline and duration of the test, and the hours of operation and testing windows.

The professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage, disruption, or disclosure of information.

Supply chain analysis, right to audit clause, and due diligence are not related to the terms of a test with a third-party penetration tester. Supply chain analysis is the process of evaluating the security and risk posture of the suppliers and partners in a business network. Right to audit clause is a provision in a contract that gives one party the right to audit another party to verify their compliance with the contract terms and conditions. Due diligence is the process of identifying and addressing the cyber risks that a potential vendor or partner brings to an organization.

Reference = <https://www.yeahhub.com/every-penetration-tester-you-should-know-about-this-rules-of-engagement/>

<https://bing.com/search?q=rules+of+engagement+penetration+testing>

14. A penetration tester begins an engagement by performing port and service scans against the client environment according to the rules of engagement.

Which of the following reconnaissance types is the tester performing?

- A. Active
- B. Passive
- C. Defensive
- D. Offensive

Answer: A

Explanation:

Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information.

Reference = CompTIA Security+ Certification Exam Objectives, Domain 1.1: Given a scenario, conduct

reconnaissance using appropriate techniques and tools. CompTIA Security+ Study Guide (SY0-701), Chapter 2: Reconnaissance and Intelligence Gathering, page 47. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 1.

15. Which of the following is required for an organization to properly manage its restore process in the event of system failure?

- A. IRP
- B. DRP
- C. RPO
- D. SDLC

Answer: B

Explanation:

A disaster recovery plan (DRP) is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency.

A DRP typically includes the following elements:

A risk assessment that identifies the potential threats and impacts to the organization's critical assets and processes.

A business impact analysis that prioritizes the recovery of the most essential functions and data.

A recovery strategy that defines the roles and responsibilities of the recovery team, the resources and tools needed, and the steps to follow to restore the system.

A testing and maintenance plan that ensures the DRP is updated and validated regularly. A DRP is required for an organization to properly manage its restore process in the event of system failure, as it provides a clear and structured framework for recovering from a disaster and minimizing the downtime and data loss.

Reference = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325.

16. Which of the following vulnerabilities is associated with installing software outside of a manufacturer's approved software repository?

- A. Jailbreaking
- B. Memory injection
- C. Resource reuse
- D. Side loading

Answer: D

Explanation:

Side loading is the process of installing software outside of a manufacturer's approved software repository. This can expose the device to potential vulnerabilities, such as malware, spyware, or unauthorized access. Side loading can also bypass security controls and policies that are enforced by the manufacturer or the organization. Side loading is often done by users who want to access applications or features that are not available or allowed on their devices.

Reference = Sideload - CompTIA Security + Video Training | Interface Technical Training, Security+ (Plus) Certification | CompTIA IT Certifications, Load Balancers – CompTIA Security+ SY0-501 – 2.1, CompTIA Security+ SY0-601 Certification Study Guide.

17. A security analyst is reviewing the following logs:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

- A. Password spraying
- B. Account forgery
- C. Pass-the-hash
- D. Brute-force

Answer: A

Explanation:

Password spraying is a type of brute force attack that tries common passwords across several accounts to find a match. It is a mass trial-and-error approach that can bypass account lockout protocols. It can give hackers access to personal or business accounts and information. It is not a targeted attack, but a high-volume attack tactic that uses a dictionary or a list of popular or weak passwords¹².

The logs show that the attacker is using the same password ("password123") to attempt to log in to different accounts ("admin", "user1", "user2", etc.) on the same web server. This is a typical pattern of password spraying, as the attacker is hoping that at least one of the accounts has a weak password that matches the one they are trying. The attacker is also using a tool called Hydra, which is one of the most popular brute force tools, often used in cracking passwords for network authentication³.

Account forgery is not the correct answer, because it involves creating fake accounts or credentials to impersonate legitimate users or entities. There is no evidence of account forgery in the logs, as the attacker is not creating any new accounts or using forged credentials.

Pass-the-hash is not the correct answer, because it involves stealing a hashed user credential and using it to create a new authenticated session on the same network. Pass-the-hash does not require the attacker to know or crack the password, as they use the stored version of the password to initiate a new session⁴. The logs show that the attacker is using plain text passwords, not hashes, to try to log in to the web server.

Brute-force is not the correct answer, because it is a broader term that encompasses different types of attacks that involve trying different variations of symbols or words until the correct password is found. Password spraying is a specific type of brute force attack that uses a single common password against multiple accounts⁵. The logs show that the attacker is using password spraying, not brute force in general, to try to gain access to the web server.

Reference = 1: Password spraying: An overview of password spraying attacks ... - Norton, 2: Security: Credential Stuffing vs. Password Spraying - Baeldung, 3: Brute Force Attack: A definition + 6 types to know | Norton, 4: What is a Pass-the-Hash Attack? - CrowdStrike, 5: What is a Brute Force Attack? | Definition, Types & How It Works - Fortinet

18. An analyst is evaluating the implementation of Zero Trust principles within the data plane.

Which of the following would be most relevant for the analyst to evaluate?

- A. Secured zones
- B. Subject role

- C. Adaptive identity
- D. Threat scope reduction

Answer: D

Explanation:

The data plane, also known as the forwarding plane, is the part of the network that carries user traffic and data. It is responsible for moving packets from one device to another based on the routing and switching decisions made by the control plane. The data plane is a critical component of the Zero Trust architecture, as it is where most of the attacks and breaches occur. Therefore, implementing Zero Trust principles within the data plane can help to improve the security and resilience of the network.

One of the key principles of Zero Trust is to assume breach and minimize the blast radius and segment access. This means that the network should be divided into smaller and isolated segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot easily move laterally to other segments and access more resources or data. This principle is also known as threat scope reduction, as it reduces the scope and impact of a potential threat.

The other options are not as relevant for the data plane as threat scope reduction. Secured zones are a concept related to the control plane, which is the part of the network that makes routing and switching decisions. Subject role is a concept related to the identity plane, which is the part of the network that authenticates and authorizes users and devices. Adaptive identity is a concept related to the policy plane, which is the part of the network that defines and enforces the security policies and rules.

Reference = <https://bing.com/search?q=Zero+Trust+data+plane>

<https://learn.microsoft.com/en-us/security/zero-trust/deploy/data>

19. An engineer needs to find a solution that creates an added layer of security by preventing unauthorized access to internal company resources.

Which of the following would be the best solution?

- A. RDP server
- B. Jump server
- C. Proxy server
- D. Hypervisor

Answer: B

Explanation:

= A jump server is a server that acts as an intermediary between a user and a target system. A jump server can provide an added layer of security by preventing unauthorized access to internal company resources. A user can connect to the jump server using a secure protocol, such as SSH, and then access the target system from the jump server. This way, the target system is isolated from the external network and only accessible through the jump server. A jump server can also enforce security policies, such as authentication, authorization, logging, and auditing, on the user's connection. A jump server is also known as a bastion host or a jump box.

Reference = CompTIA Security+ Certification Exam Objectives, Domain 3.3: Given a scenario, implement secure network architecture concepts. CompTIA Security+ Study Guide (SY0-701), Chapter 3: Network Architecture and Design, page 101. Other Network Appliances – SY0-601 CompTIA Security+: 3.3, Video 3:03. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 2.

20. A company's web filter is configured to scan the URL for strings and deny access when matches are

found.

Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

- A. encryption=off\
- B. http://
- C. www.*.com
- D. :443

Answer: B

Explanation:

A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words “gambling”, “porn”, or “malware” in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource.

A URL typically consists of the following components: protocol://domain:port/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP. The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or 443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or ?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary.

To prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers. However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks. To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http://www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites.

The other options are not correct because they do not match the protocol of non-encrypted web traffic. Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter. https:// is the protocol of encrypted web traffic, which uses hypertext transfer protocol secure (HTTPS) to provide encryption and security for the data. www.*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol. :443 is the port number of HTTPS, which is the protocol of encrypted web traffic. Reference = CompTIA Security+ Study Guide (SY0-701), Chapter 2: Securing Networks, page 69. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

21. During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP

address from accessing the organization's network.

Which of the following fulfills this request?

- A. access-list inbound deny ig source 0.0.0.0/0 destination 10.1.4.9/32
- B. access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
- C. access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0
- D. access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32

Answer: B

Explanation:

A firewall rule is a set of criteria that determines whether to allow or deny a packet to pass through the firewall. A firewall rule consists of several elements, such as the action, the protocol, the source address, the destination address, and the port number. The syntax of a firewall rule may vary depending on the type and vendor of the firewall, but the basic logic is the same. In this question, the security analyst is creating an inbound firewall rule to block the IP address 10.1.4.9 from accessing the organization's network. This means that the action should be deny, the protocol should be any (or ig for IP), the source address should be 10.1.4.9/32 (which means a single IP address), the destination address should be 0.0.0.0/0 (which means any IP address), and the port number should be any.

Therefore, the correct firewall rule is:

```
access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
```

This rule will match any packet that has the source IP address of 10.1.4.9 and drop it. The other options are incorrect because they either have the wrong action, the wrong source address, or the wrong destination address. For example, option A has the source and destination addresses reversed, which means that it will block any packet that has the destination IP address of 10.1.4.9, which is not the intended goal. Option C has the wrong action, which is permit, which means that it will allow the packet to pass through the firewall, which is also not the intended goal.

Option D has the same problem as option A, with the source and destination addresses reversed.

Reference = Firewall Rules – CompTIA Security+ SY0-401: 1.2, Firewalls – SY0-601 CompTIA Security+: 3.3, Firewalls – CompTIA Security+ SY0-501, Understanding Firewall Rules – CompTIA Network+ N10-005: 5.5, Configuring Windows Firewall – CompTIA A+ 220-1102 – 1.6.

22. A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary.

Which of the following methods is most secure?

- A. Implementing a bastion host
- B. Deploying a perimeter network
- C. Installing a WAF
- D. Utilizing single sign-on

Answer: A

Explanation:

A bastion host is a special-purpose server that is designed to withstand attacks and provide secure access to internal resources. A bastion host is usually placed on the edge of a network, acting as a gateway or proxy to the internal network. A bastion host can be configured to allow only certain types of traffic, such as SSH or HTTP, and block all other traffic. A bastion host can also run security software such as firewalls, intrusion detection systems, and antivirus programs to monitor and filter incoming and outgoing traffic. A bastion host can provide administrative access to internal resources by requiring

strong authentication and encryption, and by logging all activities for auditing purposes¹².

A bastion host is the most secure method among the given options because it minimizes the traffic allowed through the security boundary and provides a single point of control and defense. A bastion host can also isolate the internal network from direct exposure to the internet or other untrusted networks, reducing the attack surface and the risk of compromise³.

Deploying a perimeter network is not the correct answer, because a perimeter network is a network segment that separates the internal network from the external network. A perimeter network usually hosts public-facing services such as web servers, email servers, or DNS servers that need to be accessible from the internet. A perimeter network does not provide administrative access to internal resources, but rather protects them from unauthorized access. A perimeter network can also increase the complexity and cost of network management and security⁴.

Installing a WAF is not the correct answer, because a WAF is a security tool that protects web applications from common web-based attacks by monitoring, filtering, and blocking HTTP traffic. A WAF can prevent attacks such as cross-site scripting, SQL injection, or file inclusion, among others. A WAF does not provide administrative access to internal resources, but rather protects them from web application vulnerabilities. A WAF is also not a comprehensive solution for network security, as it only operates at the application layer and does not protect against other types of attacks or threats⁵.

Utilizing single sign-on is not the correct answer, because single sign-on is a method of authentication that allows users to access multiple sites, services, or applications with one username and password. Single sign-on can simplify the sign-in process for users and reduce the number of passwords they have to remember and manage. Single sign-on does not provide administrative access to internal resources, but rather enables access to various resources that the user is authorized to use. Single sign-on can also introduce security risks if the user's credentials are compromised or if the single sign-on provider is breached⁶.

Reference = 1: Bastion host - Wikipedia, 2: 14 Best Practices to Secure SSH Bastion Host - goteleport.com, 3: The Importance Of Bastion Hosts In Network Security, 4: What is the network perimeter? | Cloudflare, 5: What is a WAF? | Web Application Firewall explained, 6: [What is single sign-on (SSO)? - Definition from WhatIs.com]

23. A security analyst is reviewing alerts in the SIEM related to potential malicious network traffic coming from an employee's corporate laptop. The security analyst has determined that additional data about the executable running on the machine is necessary to continue the investigation.

Which of the following logs should the analyst use as a data source?

- A. Application
- B. IPS/IDS
- C. Network
- D. Endpoint

Answer: D

Explanation:

An endpoint log is a file that contains information about the activities and events that occur on an end-user device, such as a laptop, desktop, tablet, or smartphone. Endpoint logs can provide valuable data for security analysts, such as the processes running on the device, the network connections established, the files accessed or modified, the user actions performed, and the applications installed or updated. Endpoint logs can also record the details of any executable files running on the device, such as the

name, path, size, hash, signature, and permissions of the executable.

An application log is a file that contains information about the events that occur within a software application, such as errors, warnings, transactions, or performance metrics. Application logs can help developers and administrators troubleshoot issues, optimize performance, and monitor user behavior. However, application logs may not provide enough information about the executable files running on the device, especially if they are malicious or unknown.

An IPS/IDS log is a file that contains information about the network traffic that is monitored and analyzed by an intrusion prevention system (IPS) or an intrusion detection system (IDS). IPS/IDS logs can help security analysts identify and block potential attacks, such as exploit attempts, denial-of-service (DoS) attacks, or malicious scans. However, IPS/IDS logs may not provide enough information about the executable files running on the device, especially if they are encrypted, obfuscated, or use legitimate protocols.

A network log is a file that contains information about the network activity and communication that occurs between devices, such as IP addresses, ports, protocols, packets, or bytes. Network logs can help security analysts understand the network topology, traffic patterns, and bandwidth usage.

However, network logs may not provide enough information about the executable files running on the device, especially if they are hidden, spoofed, or use proxy servers.

Therefore, the best log type to use as a data source for additional information about the executable running on the machine is the endpoint log, as it can provide the most relevant and detailed data about the executable file and its behavior.

Reference = <https://www.crowdstrike.com/cybersecurity-101/observability/application-log/>
<https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging>

24. A cyber operations team informs a security analyst about a new tactic malicious actors are using to compromise networks.

SIEM alerts have not yet been configured.

Which of the following best describes what the security analyst should do to identify this behavior?

- A. [Digital forensics
- B. E-discovery
- C. Incident response
- D. Threat hunting

Answer: D

Explanation:

Threat hunting is the process of proactively searching for signs of malicious activity or compromise in a network, rather than waiting for alerts or indicators of compromise (IOCs) to appear. Threat hunting can help identify new tactics, techniques, and procedures (TTPs) used by malicious actors, as well as uncover hidden or stealthy threats that may have evaded detection by security tools. Threat hunting requires a combination of skills, tools, and methodologies, such as hypothesis generation, data collection and analysis, threat intelligence, and incident response. Threat hunting can also help improve the security posture of an organization by providing feedback and recommendations for security improvements.

Reference = CompTIA Security+ Certification Exam Objectives, Domain 4.1: Given a scenario, analyze potential indicators of malicious activity. CompTIA Security+ Study Guide (SY0-701), Chapter 4: Threat Detection and Response, page 153. Threat Hunting – SY0-701 CompTIA Security+: 4.1, Video 3:18.

CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 3.

25. A company purchased cyber insurance to address items listed on the risk register.

Which of the following strategies does this represent?

- A. Accept
- B. Transfer
- C. Mitigate
- D. Avoid

Answer: B

Explanation:

Cyber insurance is a type of insurance that covers the financial losses and liabilities that result from cyberattacks, such as data breaches, ransomware, denial-of-service, phishing, or malware. Cyber insurance can help a company recover from the costs of restoring data, repairing systems, paying ransoms, compensating customers, or facing legal actions. Cyber insurance is one of the possible strategies that a company can use to address the items listed on the risk register. A risk register is a document that records the identified risks, their probability, impact, and mitigation strategies for a project or an organization.

The four common risk mitigation strategies are:

Accept: The company acknowledges the risk and decides to accept the consequences without taking any action to reduce or eliminate the risk. This strategy is usually chosen when the risk is low or the cost of mitigation is too high.

Transfer: The company transfers the risk to a third party, such as an insurance company, a vendor, or a partner. This strategy is usually chosen when the risk is high or the company lacks the resources or expertise to handle the risk.

Mitigate: The company implements controls or measures to reduce the likelihood or impact of the risk. This strategy is usually chosen when the risk is moderate or the cost of mitigation is reasonable.

Avoid: The company eliminates the risk by changing the scope, plan, or design of the project or the organization. This strategy is usually chosen when the risk is unacceptable or the cost of mitigation is too high.

By purchasing cyber insurance, the company is transferring the risk to the insurance company, which will cover the financial losses and liabilities in case of a cyberattack. Therefore, the correct answer is B.

Transfer.

Reference = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 377. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.1: Risk Management, video: Risk Mitigation Strategies (5:37).

26. A security administrator would like to protect data on employees' laptops.

Which of the following encryption techniques should the security administrator use?

- A. Partition
- B. Asymmetric
- C. Full disk
- D. Database

Answer: C

Explanation:

Full disk encryption (FDE) is a technique that encrypts all the data on a hard drive, including the operating system, applications, and files. FDE protects the data from unauthorized access in case the laptop is lost, stolen, or disposed of without proper sanitization. FDE requires the user to enter a password, a PIN, a smart card, or a biometric factor to unlock the drive and boot the system. FDE can be implemented by using software solutions, such as BitLocker, FileVault, or VeraCrypt, or by using hardware solutions, such as self-encrypting drives (SEDs) or Trusted Platform Modules (TPMs). FDE is a recommended encryption technique for laptops and other mobile devices that store sensitive data.

Partition encryption is a technique that encrypts only a specific partition or volume on a hard drive, leaving the rest of the drive unencrypted. Partition encryption is less secure than FDE, as it does not protect the entire drive and may leave traces of data on unencrypted areas. Partition encryption is also less convenient than FDE, as it requires the user to mount and unmount the encrypted partition manually.

Asymmetric encryption is a technique that uses a pair of keys, one public and one private, to encrypt and decrypt data. Asymmetric encryption is mainly used for securing communication, such as email, web, or VPN, rather than for encrypting data at rest. Asymmetric encryption is also slower and more computationally intensive than symmetric encryption, which is the type of encryption used by FDE and partition encryption.

Database encryption is a technique that encrypts data stored in a database, such as tables, columns, rows, or cells. Database encryption can be done at the application level, the database level, or the file system level. Database encryption is useful for protecting data from unauthorized access by database administrators, hackers, or malware, but it does not protect the data from physical theft or loss of the device that hosts the database.

Reference = Data Encryption – CompTIA Security+ SY0-401: 4.4, CompTIA Security+ Cheat Sheet and PDF | Zero To Mastery, CompTIA Security+ SY0-601 Certification Course - Cybr, Application Hardening – SY0-601 CompTIA Security+: 3.2.

27. Which of the following security control types does an acceptable use policy best represent?

- A. Detective
- B. Compensating
- C. Corrective
- D. Preventive

Answer: D

Explanation:

An acceptable use policy (AUP) is a set of rules that govern how users can access and use a corporate network or the internet. The AUP helps companies minimize their exposure to cyber security threats and limit other risks. The AUP also serves as a notice to users about what they are not allowed to do and protects the company against misuse of their network. Users usually have to acknowledge that they understand and agree to the rules before accessing the network¹.

An AUP best represents a preventive security control type, because it aims to deter or stop potential security incidents from occurring in the first place. A preventive control is proactive and anticipates possible threats and vulnerabilities, and implements measures to prevent them from exploiting or harming the system or the data. A preventive control can be physical, technical, or administrative in nature².

Some examples of preventive controls are:

Locks, fences, or guards that prevent unauthorized physical access to a facility or a device

Firewalls, antivirus software, or encryption that prevent unauthorized logical access to a network or a system

Policies, procedures, or training that prevent unauthorized or inappropriate actions or behaviors by users or employees

An AUP is an example of an administrative preventive control, because it defines the policies and procedures that users must follow to ensure the security and proper use of the network and the IT resources. An AUP can prevent users from engaging in activities that could compromise the security, performance, or availability of the network or the system, such as:

Downloading or installing unauthorized or malicious software

Accessing or sharing sensitive or confidential information without authorization or encryption

Using the network or the system for personal, illegal, or unethical purposes

Bypassing or disabling security controls or mechanisms

Connecting unsecured or unapproved devices to the network

By enforcing an AUP, a company can prevent or reduce the likelihood of security breaches, data loss, legal liability, or reputational damage caused by user actions or inactions³.

Reference = 1: How to Create an Acceptable Use Policy - CoreTech, 2: [Security Control Types: Preventive, Detective, Corrective, and Compensating], 3: Why You Need A Corporate Acceptable Use Policy - CompTIA

28. An IT manager informs the entire help desk staff that only the IT manager and the help desk lead will have access to the administrator console of the help desk software.

Which of the following security techniques is the IT manager setting up?

A. Hardening

B. Employee monitoring

C. Configuration enforcement

D. Least privilege

Answer: D

Explanation:

The principle of least privilege is a security concept that limits access to resources to the minimum level needed for a user, a program, or a device to perform a legitimate function. It is a cybersecurity best practice that protects high-value data and assets from compromise or insider threat. Least privilege can be applied to different abstraction layers of a computing environment, such as processes, systems, or connected devices. However, it is rarely implemented in practice.

In this scenario, the IT manager is setting up the principle of least privilege by restricting access to the administrator console of the help desk software to only two authorized users: the IT manager and the help desk lead. This way, the IT manager can prevent unauthorized or accidental changes to the software configuration, data, or functionality by other help desk staff. The other help desk staff will only have access to the normal user interface of the software, which is sufficient for them to perform their job functions.

The other options are not correct. Hardening is the process of securing a system by reducing its surface of vulnerability, such as by removing unnecessary software, changing default passwords, or disabling unnecessary services. Employee monitoring is the surveillance of workers' activity, such as by tracking web browsing, application use, keystrokes, or screenshots. Configuration enforcement is the process of

ensuring that a system adheres to a predefined set of security settings, such as by applying a patch, a policy, or a template.

Reference =

https://en.wikipedia.org/wiki/Principle_of_least_privilege

https://en.wikipedia.org/wiki/Principle_of_least_privilege

29. Which of the following is the most likely to be used to document risks, responsible parties, and thresholds?

- A. Risk tolerance
- B. Risk transfer
- C. Risk register
- D. Risk analysis

Answer: C

Explanation:

A risk register is a document that records and tracks the risks associated with a project, system, or organization. A risk register typically includes information such as the risk description, the risk owner, the risk probability, the risk impact, the risk level, the risk response strategy, and the risk status. A risk register can help identify, assess, prioritize, monitor, and control risks, as well as communicate them to relevant stakeholders. A risk register can also help document the risk tolerance and thresholds of an organization, which are the acceptable levels of risk exposure and the criteria for escalating or mitigating risks.

Reference = CompTIA Security+ Certification Exam Objectives, Domain 5.1: Explain the importance of policies, plans, and procedures related to organizational security. CompTIA Security+ Study Guide (SY0-701), Chapter 5: Governance, Risk, and Compliance, page 211. CompTIA Security+ Certification Guide, Chapter 2: Risk Management, page 33. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 4.

30. Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

- A. Disaster recovery plan
- B. Incident response procedure
- C. Business continuity plan
- D. Change management procedure

Answer: D

Explanation:

A change management procedure is a set of steps and guidelines that a security administrator should adhere to when setting up a new set of firewall rules. A firewall is a device or software that can filter, block, or allow network traffic based on predefined rules or policies. A firewall rule is a statement that defines the criteria and action for a firewall to apply to a packet or a connection. For example, a firewall rule can allow or deny traffic based on the source and destination IP addresses, ports, protocols, or applications. Setting up a new set of firewall rules is a type of change that can affect the security, performance, and functionality of the network. Therefore, a change management procedure is necessary to ensure that the change is planned, tested, approved, implemented, documented, and reviewed in a controlled and consistent manner. A change management procedure typically includes the following

elements:

A change request that describes the purpose, scope, impact, and benefits of the change, as well as the roles and responsibilities of the change owner, implementer, and approver.

A change assessment that evaluates the feasibility, risks, costs, and dependencies of the change, as well as the alternatives and contingency plans.

A change approval that authorizes the change to proceed to the implementation stage, based on the criteria and thresholds defined by the change policy.

A change implementation that executes the change according to the plan and schedule, and verifies the results and outcomes of the change.

A change documentation that records the details and status of the change, as well as the lessons learned and best practices.

A change review that monitors and measures the performance and effectiveness of the change, and identifies any issues or gaps that need to be addressed or improved.

A change management procedure is important for a security administrator to adhere to when setting up a new set of firewall rules, as it can help to achieve the following objectives:

Enhance the security posture and compliance of the network by ensuring that the firewall rules are aligned with the security policies and standards, and that they do not introduce any vulnerabilities or conflicts.

Minimize the disruption and downtime of the network by ensuring that the firewall rules are tested and validated before deployment, and that they do not affect the availability or functionality of the network services or applications.

Improve the efficiency and quality of the network by ensuring that the firewall rules are optimized and updated according to the changing needs and demands of the network users and stakeholders, and that they do not cause any performance or compatibility issues.

Increase the accountability and transparency of the network by ensuring that the firewall rules are documented and reviewed regularly, and that they are traceable and auditable by the relevant authorities and parties.

The other options are not correct because they are not related to the process of setting up a new set of firewall rules. A disaster recovery plan is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. An incident response procedure is a set of steps and guidelines that aim to contain, analyze, eradicate, and recover from a security incident, such as a cyberattack, data breach, or malware infection. A business continuity plan is a set of strategies and actions that aim to maintain the essential functions and operations of an organization during and after a disruptive event, such as a pandemic, power outage, or civil unrest.

Reference = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.3: Security Operations, video: Change Management (5:45).

31. A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered.

Which of the following best describes the program the company is setting up?

A. Open-source intelligence

- B. Bug bounty
- C. Red team
- D. Penetration testing

Answer: B

Explanation:

A bug bounty is a program that rewards security researchers for finding and reporting vulnerabilities in an application or system. Bug bounties are often used by companies to improve their security posture and incentivize ethical hacking. A bug bounty program typically defines the scope, rules, and compensation for the researchers.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 10. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2.

32. Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

- A. Insider
- B. Unskilled attacker
- C. Nation-state
- D. Hacktivist

Answer: C

Explanation:

A nation-state is a threat actor that is sponsored by a government or a political entity to conduct cyberattacks against other countries or organizations. Nation-states have large financial resources, advanced technical skills, and strategic objectives that may target critical systems such as military, energy, or infrastructure. Nation-states are often motivated by espionage, sabotage, or warfare¹².

Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Threat Actors – CompTIA Security+ SY0-701 – 2.1, video by Professor Messer.

33. Which of the following enables the use of an input field to run commands that can view or manipulate data?

- A. Cross-site scripting
- B. Side loading
- C. Buffer overflow
- D. SQL injection

Answer: D

Explanation:

= SQL injection is a type of attack that enables the use of an input field to run commands that can view or manipulate data in a database. SQL stands for Structured Query Language, which is a language used to communicate with databases. By injecting malicious SQL statements into an input field, an attacker can bypass authentication, access sensitive information, modify or delete data, or execute commands on the server. SQL injection is one of the most common and dangerous web application vulnerabilities.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 195. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1, page 8.

34. Employees in the research and development business unit receive extensive training to ensure they understand how to best protect company data.

Which of the following is the type of data these employees are most likely to use in day-to-day work activities?

- A. Encrypted
- B. Intellectual property
- C. Critical
- D. Data in transit

Answer: B

Explanation:

Intellectual property is a type of data that consists of ideas, inventions, designs, or other creative works that have commercial value and are protected by law. Employees in the research and development business unit are most likely to use intellectual property data in their day-to-day work activities, as they are involved in creating new products or services for the company. Intellectual property data needs to be protected from unauthorized use, disclosure, or theft, as it can give the company a competitive advantage in the market. Therefore, these employees receive extensive training to ensure they understand how to best protect this type of data.

Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 90; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 1.2 - Security Concepts, 7:57 - 9:03.

35. A company has begun labeling all laptops with asset inventory stickers and associating them with employee IDs.

Which of the following security benefits do these actions provide? (Choose two.)

- A. If a security incident occurs on the device, the correct employee can be notified.
- B. The security team will be able to send user awareness training to the appropriate device.
- C. Users can be mapped to their devices when configuring software MFA tokens.
- D. User-based firewall policies can be correctly targeted to the appropriate laptops.
- E. When conducting penetration testing, the security team will be able to target the desired laptops.
- F. Company data can be accounted for when the employee leaves the organization.

Answer: A, F

Explanation:

Labeling all laptops with asset inventory stickers and associating them with employee IDs can provide several security benefits for a company.

Two of these benefits are:

- A. If a security incident occurs on the device, the correct employee can be notified. An asset inventory sticker is a label that contains a unique identifier for a laptop, such as a serial number, a barcode, or a QR code. By associating this identifier with an employee ID, the security team can easily track and locate the owner of the laptop in case of a security incident, such as a malware infection, a data breach, or a theft. This way, the security team can notify the correct employee about the incident, and provide them with the necessary instructions or actions to take, such as changing passwords, scanning for viruses, or reporting the loss. This can help to contain the incident, minimize the damage, and prevent further escalation.
- F. Company data can be accounted for when the employee leaves the organization. When an employee

leaves the organization, the company needs to ensure that all the company data and assets are returned or deleted from the employee's laptop. By labeling the laptop with an asset inventory sticker and associating it with an employee ID, the company can easily identify and verify the laptop that belongs to the departing employee, and perform the appropriate data backup, wipe, or transfer procedures. This can help to protect the company data from unauthorized access, disclosure, or misuse by the former employee or any other party.

The other options are not correct because they are not related to the security benefits of labeling laptops with asset inventory stickers and associating them with employee IDs.

B. The security team will be able to send user awareness training to the appropriate device. User awareness training is a type of security education that aims to improve the knowledge and behavior of users regarding security threats and best practices. The security team can send user awareness training to the appropriate device by using the email address, username, or IP address of the device, not the asset inventory sticker or the employee ID.

C. Users can be mapped to their devices when configuring software MFA tokens. Software MFA tokens are a type of multi-factor authentication that uses a software application to generate a one-time password or a push notification for verifying the identity of a user. Users can be mapped to their devices when configuring software MFA tokens by using the device ID, phone number, or email address of the device, not the asset inventory sticker or the employee ID.

D. User-based firewall policies can be correctly targeted to the appropriate laptops. User-based firewall policies are a type of firewall rules that apply to specific users or groups of users, regardless of the device or location they use to access the network. User-based firewall policies can be correctly targeted to the appropriate laptops by using the username, domain, or certificate of the user, not the asset inventory sticker or the employee ID.

E. When conducting penetration testing, the security team will be able to target the desired laptops. Penetration testing is a type of security assessment that simulates a real-world attack on a network or system to identify and exploit vulnerabilities. When conducting penetration testing, the security team will be able to target the desired laptops by using the IP address, hostname, or MAC address of the laptop, not the asset inventory sticker or the employee ID.

Reference = CompTIA Security+ Study Guide (SY0-701), Chapter 1: General Security Concepts, page 17. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.4: Asset Management, video: Asset Inventory (6:12).

36. A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work.

Which of the following is the best option?

- A. Send out periodic security reminders.
- B. Update the content of new hire documentation.
- C. Modify the content of recurring training.
- D. Implement a phishing campaign

Answer: C

Explanation:

Recurring training is a type of security awareness training that is conducted periodically to refresh and update the knowledge and skills of the users. Recurring training can help improve the situational and environmental awareness of existing users as they transition from remote to in-office work, as it can

cover the latest threats, best practices, and policies that are relevant to their work environment.

Modifying the content of recurring training can ensure that the users are aware of the current security landscape and the expectations of their roles.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 232. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

37. A newly appointed board member with cybersecurity knowledge wants the board of directors to receive a quarterly report detailing the number of incidents that impacted the organization. The systems administrator is creating a way to present the data to the board of directors.

Which of the following should the systems administrator use?

- A. Packet captures
- B. Vulnerability scans
- C. Metadata
- D. Dashboard

Answer: D

Explanation:

A dashboard is a graphical user interface that provides a visual representation of key performance indicators, metrics, and trends related to security events and incidents. A dashboard can help the board of directors to understand the number and impact of incidents that affected the organization in a given period, as well as the status and effectiveness of the security controls and processes. A dashboard can also allow the board of directors to drill down into specific details or filter the data by various criteria¹².

A packet capture is a method of capturing and analyzing the network traffic that passes through a device or a network segment. A packet capture can provide detailed information about the source, destination, protocol, and content of each packet, but it is not a suitable way to present a summary of incidents to the board of directors¹³.

A vulnerability scan is a process of identifying and assessing the weaknesses and exposures in a system or a network that could be exploited by attackers. A vulnerability scan can help the organization to prioritize and remediate the risks and improve the security posture, but it is not a relevant way to report the number of incidents that occurred in a quarter¹⁴.

Metadata is data that describes other data, such as its format, origin, structure, or context. Metadata can provide useful information about the characteristics and properties of data, but it is not a meaningful way to communicate the impact and frequency of incidents to the board of directors.

Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 3722: SIEM Dashboards – SY0-601 CompTIA Security+: 4.3, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 3464: CompTIA Security+ SY0-701 Certification Study Guide, page 362.: CompTIA Security+ SY0-701 Certification Study Guide, page 97.

38. A systems administrator receives the following alert from a file integrity monitoring tool:

The hash of the cmd.exe file has changed.

The systems administrator checks the OS logs and notices that no patches were applied in the last two months.

Which of the following most likely occurred?

- A. The end user changed the file permissions.

- B. A cryptographic collision was detected.
- C. A snapshot of the file system was taken.
- D. A rootkit was deployed.

Answer: D

Explanation:

A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity. A rootkit can change the hash of the cmd.exe file, which is a command-line interpreter for Windows systems, to avoid detection by antivirus or file integrity monitoring tools. A rootkit can also grant the attacker remote access and control over the infected system, as well as perform malicious actions such as stealing data, installing backdoors, or launching attacks on other systems. A rootkit is one of the most difficult types of malware to remove, as it can persist even after rebooting or reinstalling the OS. Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 147. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2, page 9.

39. Which of the following roles, according to the shared responsibility model, is responsible for securing the company's database in an IaaS model for a cloud environment?
- A. Client
 - B. Third-party vendor
 - C. Cloud provider
 - D. DBA

Answer: A

Explanation:

According to the shared responsibility model, the client and the cloud provider have different roles and responsibilities for securing the cloud environment, depending on the service model. In an IaaS (Infrastructure as a Service) model, the cloud provider is responsible for securing the physical infrastructure, such as the servers, storage, and network devices, while the client is responsible for securing the operating systems, applications, and data that run on the cloud infrastructure. Therefore, the client is responsible for securing the company's database in an IaaS model for a cloud environment, as the database is an application that stores data. The client can use various security controls, such as encryption, access control, backup, and auditing, to protect the database from unauthorized access, modification, or loss. The third-party vendor and the DBA (Database Administrator) are not roles defined by the shared responsibility model, but they may be involved in the implementation or management of the database security.

Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 263-264; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 5:00 - 7:40.

40. A client asked a security company to provide a document outlining the project, the cost, and the completion time frame.
- Which of the following documents should the company provide to the client?
- A. MSA
 - B. SLA
 - C. BPA
 - D. SOW

Answer: D

Explanation:

An ISOW is a document that outlines the project, the cost, and the completion time frame for a security company to provide a service to a client. ISOW stands for Information Security Operations Work, and it is a type of contract that specifies the scope, deliverables, milestones, and payment terms of a security project. An ISOW is usually used for one-time or short-term projects that have a clear and defined objective and outcome. For example, an ISOW can be used for a security assessment, a penetration test, a security audit, or a security training.

The other options are not correct because they are not documents that outline the project, the cost, and the completion time frame for a security company to provide a service to a client. A MSA is a master service agreement, which is a type of contract that establishes the general terms and conditions for a long-term or ongoing relationship between a security company and a client. A MSA does not specify the details of each individual project, but rather sets the framework for future projects that will be governed by separate statements of work (SOWs). A SLA is a service level agreement, which is a type of contract that defines the quality and performance standards for a security service provided by a security company to a client. A SLA usually includes the metrics, targets, responsibilities, and penalties for measuring and ensuring the service level. A BPA is a business partnership agreement, which is a type of contract that establishes the roles and expectations for a strategic alliance between two or more security companies that collaborate to provide a joint service to a client. A BPA usually covers the objectives, benefits, risks, and obligations of the partnership.

Reference = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 387. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.2: Compliance and Controls, video: Contracts and Agreements (5:12).

41. A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting.

Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

- A. Secure cookies
- B. Version control
- C. Input validation
- D. Code signing

Answer: C

Explanation:

Input validation is a technique that checks the user input for any malicious or unexpected data before processing it by the web application. Input validation can prevent cross-site scripting (XSS) attacks, which exploit the vulnerability of a web application to execute malicious scripts in the browser of a victim. XSS attacks can compromise the confidentiality, integrity, and availability of the web application and its users. Input validation can be implemented on both the client-side and the server-side, but server-side validation is more reliable and secure. Input validation can use various methods, such as whitelisting, blacklisting, filtering, escaping, encoding, and sanitizing the input data.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 70. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2,

page 11. Application Security – SY0-601 CompTIA Security+: 3.2

42. Which of the following must be considered when designing a high-availability network? (Choose two).

- A. Ease of recovery
- B. Ability to patch
- C. Physical isolation
- D. Responsiveness
- E. Attack surface
- F. Extensible authentication

Answer: A, E

Explanation:

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption. A high-availability network must consider the following factors¹²:

Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.

Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.

The other options are not directly related to high-availability network design:

Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.

Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.

Responsiveness: This refers to the speed and quality of the network's performance and service delivery. Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss.

Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.

Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.

Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability – CompTIA Security+ SY0-701 – 3.4, video by Professor Messer.

43. A technician needs to apply a high-priority patch to a production system.

Which of the following steps should be taken first?

- A. Air gap the system.
- B. Move the system to a different network segment.
- C. Create a change control request.
- D. Apply the patch to the system.

Answer: C

Explanation:

= A change control request is a document that describes the proposed change to a system, the reason for the change, the expected impact, the approval process, the testing plan, the implementation plan, the rollback plan, and the communication plan. A change control request is a best practice for applying any patch to a production system, especially a high-priority one, as it ensures that the change is authorized, documented, tested, and communicated. A change control request also minimizes the risk of unintended consequences, such as system downtime, data loss, or security breaches.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 235. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.1, page 13.

44. Which of the following describes the reason root cause analysis should be conducted as part of incident response?

- A. To gather IoCs for the investigation
- B. To discover which systems have been affected
- C. To eradicate any trace of malware on the network
- D. To prevent future incidents of the same nature

Answer: D

Explanation:

Root cause analysis is a process of identifying and resolving the underlying factors that led to an incident. By conducting root cause analysis as part of incident response, security professionals can learn from the incident and implement corrective actions to prevent future incidents of the same nature. For example, if the root cause of a data breach was a weak password policy, the security team can enforce a stronger password policy and educate users on the importance of password security. Root cause analysis can also help to improve security processes, policies, and procedures, and to enhance security awareness and culture within the organization. Root cause analysis is not meant to gather IoCs (indicators of compromise) for the investigation, as this is a task performed during the identification and analysis phases of incident response. Root cause analysis is also not meant to discover which systems have been affected or to eradicate any trace of malware on the network, as these are tasks performed during the containment and eradication phases of incident response.

Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 424-425; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.1 - Incident Response, 9:55 - 11:18.

45. Which of the following is the most likely outcome if a large bank fails an internal PCI DSS compliance assessment?

- A. Fines
- B. Audit findings
- C. Sanctions
- D. Reputation damage

Answer: A

Explanation:

PCI DSS is the Payment Card Industry Data Security Standard, which is a set of security requirements for organizations that store, process, or transmit cardholder data. PCI DSS aims to protect the confidentiality, integrity, and availability of cardholder data and prevent fraud, identity theft, and data

breaches. PCI DSS is enforced by the payment card brands, such as Visa, Mastercard, American Express, Discover, and JCB, and applies to all entities involved in the payment card ecosystem, such as merchants, acquirers, issuers, processors, service providers, and payment applications.

If a large bank fails an internal PCI DSS compliance assessment, the most likely outcome is that the bank will face fines from the payment card brands. An internal PCI DSS compliance assessment is a self-assessment that the bank performs to evaluate its own compliance with the PCI DSS requirements. The bank must submit the results of the internal assessment to the payment card brands or their designated agents, such as acquirers or qualified security assessors (QSAs). If the internal assessment reveals that the bank is not compliant with the PCI DSS requirements, the payment card brands may impose fines on the bank as a penalty for violating the PCI DSS contract. The amount and frequency of the fines may vary depending on the severity and duration of the non-compliance, the number and type of cardholder data compromised, and the level of cooperation and remediation from the bank. The fines can range from thousands to millions of dollars per month, and can increase over time if the non-compliance is not resolved.

The other options are not correct because they are not the most likely outcomes if a large bank fails an internal PCI DSS compliance assessment.

B. Audit findings. Audit findings are the results of an external PCI DSS compliance assessment that is performed by a QSA or an approved scanning vendor (ASV). An external assessment is required for certain entities that handle a large volume of cardholder data or have a history of non-compliance. An external assessment may also be triggered by a security incident or a request from the payment card brands. Audit findings may reveal the gaps and weaknesses in the bank's security controls and recommend corrective actions to achieve compliance. However, audit findings are not the outcome of an internal assessment, which is performed by the bank itself.

C. Sanctions. Sanctions are the measures that the payment card brands may take against the bank if the bank fails to pay the fines or comply with the PCI DSS requirements. Sanctions may include increasing the fines, suspending or terminating the bank's ability to accept or process payment cards, or revoking the bank's PCI DSS certification. Sanctions are not the immediate outcome of an internal assessment, but rather the possible consequence of prolonged or repeated non-compliance.

D. Reputation damage. Reputation damage is the loss of trust and credibility that the bank may suffer from its customers, partners, regulators, and the public if the bank fails an internal PCI DSS compliance assessment. Reputation damage may affect the bank's brand image, customer loyalty, market share, and profitability. Reputation damage is not a direct outcome of an internal assessment, but rather a potential risk that the bank may face if the non-compliance is exposed or exploited by malicious actors.

Reference = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 388. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.2: Compliance and Controls, video: PCI DSS (5:12). PCI Security Standards Council, PCI DSS Quick Reference Guide, page 4. PCI Security Standards Council, PCI DSS FAQs, question 8. PCI Security Standards Council, PCI DSS FAQs, question 9. [PCI Security Standards Council], PCI DSS FAQs, question 10. [PCI Security Standards Council], PCI DSS FAQs, question 11. [PCI Security Standards Council], PCI DSS FAQs, question 12. [PCI Security Standards Council], PCI DSS FAQs, question 13. [PCI Security Standards Council], PCI DSS FAQs, question 14. [PCI Security Standards Council], PCI DSS FAQs, question 15. [PCI Security Standards Council], PCI DSS FAQs, question 16. [PCI Security Standards Council], PCI DSS FAQs, question 17. [PCI Security Standards Council], PCI DSS FAQs, question 18. [PCI Security Standards Council], PCI DSS FAQs, question 19. [PCI Security Standards

Council], PCI DSS FAQs, question 20. [PCI Security Standards Council], PCI DSS FAQs, question 21. [PCI Security Standards Council], PCI DSS FAQs, question 22. [PCI Security Standards Council], PCI DSS FAQs, question 23. [PCI Security Standards Council], PCI DSS FAQs, question 24. [PCI Security Standards Council], PCI DSS FAQs, question 25. [PCI Security Standards Council], PCI DSS FAQs, question 26. [PCI Security Standards Council], PCI DSS FAQs, question 27. [PCI Security Standards Council], PCI DSS FAQs, question 28. [PCI Security Standards Council], PCI DSS FAQs, question 29. [PCI Security Standards Council], PCI DSS FAQs, question 30. [PCI Security Standards Council]

46. A company is developing a business continuity strategy and needs to determine how many staff members would be required to sustain the business in the case of a disruption.

Which of the following best describes this step?

- A. Capacity planning
- B. Redundancy
- C. Geographic dispersion
- D. Tablet exercise

Answer: A

Explanation:

Capacity planning is the process of determining the resources needed to meet the current and future demands of an organization. Capacity planning can help a company develop a business continuity strategy by estimating how many staff members would be required to sustain the business in the case of a disruption, such as a natural disaster, a cyberattack, or a pandemic. Capacity planning can also help a company optimize the use of its resources, reduce costs, and improve performance.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 184. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 4.1, page 14. Business Continuity – SY0-601 CompTIA Security+: 4.1

47. A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries.

Which of the following is the most effective way to limit this access?

- A. Data masking
- B. Encryption
- C. Geolocation policy
- D. Data sovereignty regulation

Answer: C

Explanation:

A geolocation policy is a policy that restricts or allows access to data or resources based on the geographic location of the user or device. A geolocation policy can be implemented using various methods, such as IP address filtering, GPS tracking, or geofencing. A geolocation policy can help the company's legal department to prevent unauthorized access to sensitive documents from individuals in high-risk countries¹².

The other options are not effective ways to limit access based on location:

Data masking: This is a technique of obscuring or replacing sensitive data with fictitious or anonymized data. Data masking can protect the privacy and confidentiality of data, but it does not prevent access to data based on location³.

Encryption: This is a process of transforming data into an unreadable format using a secret key or algorithm. Encryption can protect the integrity and confidentiality of data, but it does not prevent access to data based on location. Encryption can also be bypassed by attackers who have the decryption key or method.

Data sovereignty regulation: This is a set of laws or rules that govern the storage, processing, and transfer of data within a specific jurisdiction or country. Data sovereignty regulation can affect the availability and compliance of data, but it does not prevent access to data based on location. Data sovereignty regulation can also vary depending on the country or region.

Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: Account Policies – SY0-601 CompTIA Security+: 3.7, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 1004: CompTIA Security+ SY0-701 Certification Study Guide, page 101.: CompTIA Security+ SY0-701 Certification Study Guide, page 102.

48. Which of the following is a hardware-specific vulnerability?

- A. Firmware version
- B. Buffer overflow
- C. SQL injection
- D. Cross-site scripting

Answer: A

Explanation:

Firmware is a type of software that is embedded in a hardware device, such as a router, a printer, or a BIOS chip. Firmware controls the basic functions and operations of the device, and it can be updated or modified by the manufacturer or the user. Firmware version is a hardware-specific vulnerability, as it can expose the device to security risks if it is outdated, corrupted, or tampered with. An attacker can exploit firmware vulnerabilities to gain unauthorized access, modify device settings, install malware, or cause damage to the device or the network. Therefore, it is important to keep firmware updated and verify its integrity and authenticity.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 67. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.1, page 10.

49. While troubleshooting a firewall configuration, a technician determines that a “deny any” policy should be added to the bottom of the ACL. The technician updates the policy, but the new policy causes several company servers to become unreachable.

Which of the following actions would prevent this issue?

- A. Documenting the new policy in a change request and submitting the request to change management
- B. Testing the policy in a non-production environment before enabling the policy in the production network
- C. Disabling any intrusion prevention signatures on the 'deny any' policy prior to enabling the new policy
- D. Including an 'allow any' policy above the 'deny any' policy

Answer: B

Explanation:

A firewall policy is a set of rules that defines what traffic is allowed or denied on a network. A firewall policy should be carefully designed and tested before being implemented, as a misconfigured policy can cause network disruptions or security breaches. A common best practice is to test the policy in a non-

production environment, such as a lab or a simulation, before enabling the policy in the production network. This way, the technician can verify the functionality and performance of the policy, and identify and resolve any issues or conflicts, without affecting the live network. Testing the policy in a non-production environment would prevent the issue of the 'deny any' policy causing several company servers to become unreachable, as the technician would be able to detect and correct the problem before applying the policy to the production network.

Documenting the new policy in a change request and submitting the request to change management is a good practice, but it would not prevent the issue by itself. Change management is a process that ensures that any changes to the network are authorized, documented, and communicated, but it does not guarantee that the changes are error-free or functional. The technician still needs to test the policy before implementing it.

Disabling any intrusion prevention signatures on the 'deny any' policy prior to enabling the new policy would not prevent the issue, and it could reduce the security of the network. Intrusion prevention signatures are patterns that identify malicious or unwanted traffic, and allow the firewall to block or alert on such traffic. Disabling these signatures would make the firewall less effective in detecting and preventing attacks, and it would not affect the reachability of the company servers.

Including an 'allow any' policy above the 'deny any' policy would not prevent the issue, and it would render the 'deny any' policy useless. A firewall policy is processed from top to bottom, and the first matching rule is applied. An 'allow any' policy would match any traffic and allow it to pass through the firewall, regardless of the source, destination, or protocol. This would negate the purpose of the 'deny any' policy, which is to block any traffic that does not match any of the previous rules. Moreover, an 'allow any' policy would create a security risk, as it would allow any unauthorized or malicious traffic to enter or exit the network.

Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 204-205; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 2.1 - Network Security Devices, 8:00 - 10:00.

50. An organization is building a new backup data center with cost-benefit as the primary requirement and RTO and RPO values around two days.

Which of the following types of sites is the best for this scenario?

- A. Real-time recovery
- B. Hot
- C. Cold
- D. Warm

Answer: C

Explanation:

A cold site is a type of backup data center that has the necessary infrastructure to support IT operations, but does not have any pre-configured hardware or software. A cold site is the cheapest option among the backup data center types, but it also has the longest recovery time objective (RTO) and recovery point objective (RPO) values. A cold site is suitable for scenarios where the cost-benefit is the primary requirement and the RTO and RPO values are not very stringent. A cold site can take up to two days or more to restore the normal operations after a disaster.

Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 387; Backup Types – SY0-601 CompTIA Security+: 2.5, video at 4:50.

51. A company requires hard drives to be securely wiped before sending decommissioned systems to recycling.

Which of the following best describes this policy?

- A. Enumeration
- B. Sanitization
- C. Destruction
- D. Inventory

Answer: B

Explanation:

Sanitization is the process of removing sensitive data from a storage device or a system before it is disposed of or reused. Sanitization can be done by using software tools or hardware devices that overwrite the data with random patterns or zeros, making it unrecoverable. Sanitization is different from destruction, which is the physical damage of the storage device to render it unusable. Sanitization is also different from enumeration, which is the identification of network resources or devices, and inventory, which is the tracking of assets and their locations. The policy of securely wiping hard drives before sending decommissioned systems to recycling is an example of sanitization, as it ensures that no confidential data can be retrieved from the recycled devices.

Reference = Secure Data Destruction – SY0-601 CompTIA Security+: 2.7, video at 1:00; CompTIA Security+ SY0-701 Certification Study Guide, page 387.

52. A systems administrator works for a local hospital and needs to ensure patient data is protected and secure.

Which of the following data classifications should be used to secure patient data?

- A. Private
- B. Critical
- C. Sensitive
- D. Public

Answer: C

Explanation:

Data classification is a process of categorizing data based on its level of sensitivity, value, and impact to the organization if compromised. Data classification helps to determine the appropriate security controls and policies to protect the data from unauthorized access, disclosure, or modification. Different organizations may use different data classification schemes, but a common one is the four-tier model, which consists of the following categories: public, private, sensitive, and critical.

Public data is data that is intended for public access and disclosure, and has no impact to the organization if compromised. Examples of public data include marketing materials, press releases, and public web pages.

Private data is data that is intended for internal use only, and has a low to moderate impact to the organization if compromised. Examples of private data include employee records, financial reports, and internal policies.

Sensitive data is data that is intended for authorized use only, and has a high impact to the organization if compromised. Examples of sensitive data include personal information, health records, and intellectual property.

Critical data is data that is essential for the organization's operations and survival, and has a severe

impact to the organization if compromised. Examples of critical data include encryption keys, disaster recovery plans, and system backups.

Patient data is a type of sensitive data, as it contains personal and health information that is protected by law and ethical standards. Patient data should be used only by authorized personnel for legitimate purposes, and should be secured from unauthorized access, disclosure, or modification. Therefore, the systems administrator should use the sensitive data classification to secure patient data.

Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 90-91; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.5 - Data Classifications, 0:00 - 4:30.

53. A U.S.-based cloud-hosting provider wants to expand its data centers to new international locations. Which of the following should the hosting provider consider first?

- A. Local data protection regulations
- B. Risks from hackers residing in other countries
- C. Impacts to existing contractual obligations
- D. Time zone differences in log correlation

Answer: A

Explanation:

Local data protection regulations are the first thing that a cloud-hosting provider should consider before expanding its data centers to new international locations. Data protection regulations are laws or standards that govern how personal or sensitive data is collected, stored, processed, and transferred across borders. Different countries or regions may have different data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or the California Consumer Privacy Act (CCPA) in the United States. A cloud-hosting provider must comply with the local data protection regulations of the countries or regions where it operates or serves customers, or else it may face legal penalties, fines, or reputational damage. Therefore, a cloud-hosting provider should research and understand the local data protection regulations of the new international locations before expanding its data centers there.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 7, page 269. CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1, page 14.

54. Which of the following would be the best way to block unknown programs from executing?

- A. Access control list
- B. Application allow list.
- C. Host-based firewall
- D. DLP solution

Answer: B

Explanation:

An application allow list is a security technique that specifies which applications are permitted to run on a system or a network. An application allow list can block unknown programs from executing by only allowing the execution of programs that are explicitly authorized and verified. An application allow list can prevent malware, unauthorized software, or unwanted applications from running and compromising the security of the system or the network¹².

The other options are not the best ways to block unknown programs from executing:

Access control list: This is a security technique that specifies which users or groups are granted or

denied access to a resource or an object. An access control list can control the permissions and privileges of users or groups, but it does not directly block unknown programs from executing¹³.

Host-based firewall: This is a security device that monitors and filters the incoming and outgoing network traffic on a single host or system. A host-based firewall can block or allow network connections based on predefined rules, but it does not directly block unknown programs from executing¹.

DLP solution: This is a security system that detects and prevents the unauthorized transmission or leakage of sensitive data. A DLP solution can protect the confidentiality and integrity of data, but it does not directly block unknown programs from executing¹.

Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: Application Whitelisting – CompTIA Security+ SY0-701 – 3.5, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 98.: CompTIA Security+ SY0-701 Certification Study Guide, page 99.: CompTIA Security+ SY0-701 Certification Study Guide, page 100.

55. A company hired a consultant to perform an offensive security assessment covering penetration testing and social engineering.

Which of the following teams will conduct this assessment activity?

- A. White
- B. Purple
- C. Blue
- D. Red

Answer: D

Explanation:

A red team is a group of security professionals who perform offensive security assessments covering penetration testing and social engineering. A red team simulates real-world attacks and exploits the vulnerabilities of a target organization, system, or network. A red team aims to test the effectiveness of the security controls, policies, and procedures of the target, as well as the awareness and response of the staff and the blue team. A red team can be hired as an external consultant or formed internally within the organization.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 18. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.8, page 4. Security Teams – SY0-601 CompTIA Security+: 1.8

56. A software development manager wants to ensure the authenticity of the code created by the company.

Which of the following options is the most appropriate?

- A. Testing input validation on the user input fields
- B. Performing code signing on company-developed software
- C. Performing static code analysis on the software
- D. Ensuring secure cookies are use

Answer: B

Explanation:

Code signing is a technique that uses cryptography to verify the authenticity and integrity of the code created by the company. Code signing involves applying a digital signature to the code using a private key that only the company possesses. The digital signature can be verified by anyone who has the

corresponding public key, which can be distributed through a trusted certificate authority. Code signing can prevent unauthorized modifications, tampering, or malware injection into the code, and it can also assure the users that the code is from a legitimate source.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 74. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2, page 11. Application Security – SY0-601 CompTIA Security+: 3.2

57. Which of the following can be used to identify potential attacker activities without affecting production servers?

- A. Honey pot
- B. Video surveillance
- C. Zero Trust
- D. Geofencing

Answer: A

Explanation:

A honey pot is a system or a network that is designed to mimic a real production server and attract potential attackers. A honey pot can be used to identify the attacker's methods, techniques, and objectives without affecting the actual production servers. A honey pot can also divert the attacker's attention from the real targets and waste their time and resources¹².

The other options are not effective ways to identify potential attacker activities without affecting production servers:

Video surveillance: This is a physical security technique that uses cameras and monitors to record and observe the activities in a certain area. Video surveillance can help to deter, detect, and investigate physical intrusions, but it does not directly identify the attacker's activities on the network or the servers³.

Zero Trust: This is a security strategy that assumes that no user, device, or network is trustworthy by default and requires strict verification and validation for every request and transaction. Zero Trust can help to improve the security posture and reduce the attack surface of an organization, but it does not directly identify the attacker's activities on the network or the servers⁴.

Geofencing: This is a security technique that uses geographic location as a criterion to restrict or allow access to data or resources. Geofencing can help to protect the data sovereignty and compliance of an organization, but it does not directly identify the attacker's activities on the network or the servers⁵.

Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Honey pots and Deception – SY0-601 CompTIA Security+: 2.1, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 985: CompTIA Security+ SY0-701 Certification Study Guide, page 99.

58. During an investigation, an incident response team attempts to understand the source of an incident. Which of the following incident response activities describes this process?

- A. Analysis
- B. Lessons learned
- C. Detection
- D. Containment

Answer: A

Explanation:

Analysis is the incident response activity that describes the process of understanding the source of an incident. Analysis involves collecting and examining evidence, identifying the root cause, determining the scope and impact, and assessing the threat actor's motives and capabilities. Analysis helps the incident response team to formulate an appropriate response strategy, as well as to prevent or mitigate future incidents. Analysis is usually performed after detection and before containment, eradication, recovery, and lessons learned.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 223. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.2, page 13.

59. A security practitioner completes a vulnerability assessment on a company's network and finds several vulnerabilities, which the operations team remediates.

Which of the following should be done next?

- A. Conduct an audit.
- B. Initiate a penetration test.
- C. Rescan the network.
- D. Submit a report.

Answer: C

Explanation:

After completing a vulnerability assessment and remediating the identified vulnerabilities, the next step is to rescan the network to verify that the vulnerabilities have been successfully fixed and no new vulnerabilities have been introduced. A vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network, system, or application that could be exploited by attackers. A vulnerability assessment typically involves using automated tools, such as scanners, to scan the network and generate a report of the findings. The report may include information such as the severity, impact, and remediation of the vulnerabilities. The operations team is responsible for applying the appropriate patches, updates, or configurations to address the vulnerabilities and reduce the risk to the network. A rescan is necessary to confirm that the remediation actions have been effective and that the network is secure.

Conducting an audit, initiating a penetration test, or submitting a report are not the next steps after completing a vulnerability assessment and remediating the vulnerabilities. An audit is a process of reviewing and verifying the compliance of the network with the established policies, standards, and regulations. An audit may be performed by internal or external auditors, and it may use the results of the vulnerability assessment as part of the evidence. However, an audit is not a mandatory step after a vulnerability assessment, and it does not validate the effectiveness of the remediation actions.

A penetration test is a process of simulating a real-world attack on the network to test the security defenses and identify any gaps or weaknesses. A penetration test may use the results of the vulnerability assessment as a starting point, but it goes beyond scanning and involves exploiting the vulnerabilities to gain access or cause damage. A penetration test may be performed after a vulnerability assessment, but only with the proper authorization, scope, and rules of engagement. A penetration test is not a substitute for a rescan, as it does not verify that the vulnerabilities have been fixed.

Submitting a report is a step that is done after the vulnerability assessment, but before the remediation. The report is a document that summarizes the findings and recommendations of the vulnerability assessment, and it is used to communicate the results to the stakeholders and the operations team. The report may also include a follow-up plan and a timeline for the remediation actions. However, submitting

a report is not the final step after the remediation, as it does not confirm that the network is secure.

Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 372-375; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 0:00 - 8:00.

60. An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device.

Which of the following best describes the user's activity?

- A. Penetration testing
- B. Phishing campaign
- C. External audit
- D. Insider threat

Answer: D

Explanation:

An insider threat is a security risk that originates from within the organization, such as an employee, contractor, or business partner, who has authorized access to the organization's data and systems. An insider threat can be malicious, such as stealing, leaking, or sabotaging sensitive data, or unintentional, such as falling victim to phishing or social engineering. An insider threat can cause significant damage to the organization's reputation, finances, operations, and legal compliance. The user's activity of logging in remotely after hours and copying large amounts of data to a personal device is an example of a malicious insider threat, as it violates the organization's security policies and compromises the confidentiality and integrity of the data.

Reference = Insider Threats – CompTIA Security+ SY0-701: 3.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 133.

61. Which of the following allows for the attribution of messages to individuals?

- A. Adaptive identity
- B. Non-repudiation
- C. Authentication
- D. Access logs

Answer: B

Explanation:

Non-repudiation is the ability to prove that a message or document was sent or signed by a particular person, and that the person cannot deny sending or signing it. Non-repudiation can be achieved by using cryptographic techniques, such as hashing and digital signatures, that can verify the authenticity and integrity of the message or document. Non-repudiation can be useful for legal, financial, or contractual purposes, as it can provide evidence of the origin and content of the message or document.

Reference = Non-repudiation – CompTIA Security+ SY0-701 – 1.2, CompTIA Security+ SY0-301: 6.1 – Non-repudiation, CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.2, page 2.

62. Which of the following is the best way to consistently determine on a daily basis whether security settings on servers have been modified?

- A. Automation
- B. Compliance checklist
- C. Attestation

D. Manual audit

Answer: A

Explanation:

Automation is the best way to consistently determine on a daily basis whether security settings on servers have been modified. Automation is the process of using software, hardware, or other tools to perform tasks that would otherwise require human intervention or manual effort. Automation can help to improve the efficiency, accuracy, and consistency of security operations, as well as reduce human errors and costs. Automation can be used to monitor, audit, and enforce security settings on servers, such as firewall rules, encryption keys, access controls, patch levels, and configuration files. Automation can also alert security personnel of any changes or anomalies that may indicate a security breach or compromise¹².

The other options are not the best ways to consistently determine on a daily basis whether security settings on servers have been modified:

Compliance checklist: This is a document that lists the security requirements, standards, or best practices that an organization must follow or adhere to. A compliance checklist can help to ensure that the security settings on servers are aligned with the organizational policies and regulations, but it does not automatically detect or report any changes or modifications that may occur on a daily basis³.

Attestation: This is a process of verifying or confirming the validity or accuracy of a statement, claim, or fact. Attestation can be used to provide assurance or evidence that the security settings on servers are correct and authorized, but it does not continuously monitor or audit any changes or modifications that may occur on a daily basis⁴.

Manual audit: This is a process of examining or reviewing the security settings on servers by human inspectors or auditors. A manual audit can help to identify and correct any security issues or discrepancies on servers, but it is time-consuming, labor-intensive, and prone to human errors. A manual audit may not be feasible or practical to perform on a daily basis.

Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: Automation and Scripting – CompTIA Security+ SY0-701 – 5.1, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 98.: CompTIA Security+ SY0-701 Certification Study Guide, page 99.

63. Which of the following tools can assist with detecting an employee who has accidentally emailed a file containing a customer's PII?

- A. SCAP
- B. Net Flow
- C. Antivirus
- D. DLP

Answer: D

Explanation:

DLP stands for Data Loss Prevention, which is a tool that can assist with detecting and preventing the unauthorized transmission or leakage of sensitive data, such as a customer's PII (Personally Identifiable Information). DLP can monitor, filter, and block data in motion (such as emails), data at rest (such as files), and data in use (such as applications). DLP can also alert the sender, the recipient, or the administrator of the data breach, and apply remediation actions, such as encryption, quarantine, or deletion. DLP can help an organization comply with data protection regulations, such as GDPR, HIPAA,

or PCI DSS, and protect its reputation and assets.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 78. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5, page 11.

64. An organization recently updated its security policy to include the following statement:

Regular expressions are included in source code to remove special characters such as \$, |, ;, &, ` , and ? from variables set by forms in a web application.

Which of the following best explains the security technique the organization adopted by making this addition to the policy?

- A. Identify embedded keys
- B. Code debugging
- C. Input validation
- D. Static code analysis

Answer: C

Explanation:

Input validation is a security technique that checks the user input for any malicious or unexpected data before processing it by the application. Input validation can prevent various types of attacks, such as injection, cross-site scripting, buffer overflow, and command execution, that exploit the vulnerabilities in the application code. Input validation can be performed on both the client-side and the server-side, using methods such as whitelisting, blacklisting, filtering, sanitizing, escaping, and encoding. By including regular expressions in the source code to remove special characters from the variables set by the forms in the web application, the organization adopted input validation as a security technique. Regular expressions are patterns that match a specific set of characters or strings, and can be used to filter out any unwanted or harmful input. Special characters, such as \$, |, ;, &, ` , and ? , can be used by attackers to inject commands or scripts into the application, and cause damage or data theft. By removing these characters from the input, the organization can reduce the risk of such attacks.

Identify embedded keys, code debugging, and static code analysis are not the security techniques that the organization adopted by making this addition to the policy. Identify embedded keys is a process of finding and removing any hard-coded keys or credentials from the source code, as these can pose a security risk if exposed or compromised. Code debugging is a process of finding and fixing any errors or bugs in the source code, which can affect the functionality or performance of the application. Static code analysis is a process of analyzing the source code without executing it, to identify any vulnerabilities, flaws, or coding standards violations. These techniques are not related to the use of regular expressions to remove special characters from the input.

Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 375-376; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 8:00 - 9:08; Application Security – SY0-601 CompTIA Security+: 3.2, 0:00 - 2:00.

65. A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message.

Which of the following should the analyst do?

- A. Place posters around the office to raise awareness of common phishing activities.
- B. Implement email security filters to prevent phishing emails from being delivered

- C. Update the EDR policies to block automatic execution of downloaded programs.
- D. Create additional training for users to recognize the signs of phishing attempts.

Answer: C

Explanation:

An endpoint detection and response (EDR) system is a security tool that monitors and analyzes the activities and behaviors of endpoints, such as computers, laptops, mobile devices, and servers. An EDR system can detect, prevent, and respond to various types of threats, such as malware, ransomware, phishing, and advanced persistent threats (APTs). One of the features of an EDR system is to block the automatic execution of downloaded programs, which can prevent malicious code from running on the endpoint when a user clicks on a link in a phishing message. This can reduce the impact of a phishing attack and protect the endpoint from compromise. Updating the EDR policies to block automatic execution of downloaded programs is a technical control that can mitigate the risk of phishing, regardless of the user's awareness or behavior. Therefore, this is the best answer among the given options.

The other options are not as effective as updating the EDR policies, because they rely on administrative or physical controls that may not be sufficient to prevent or stop a phishing attack. Placing posters around the office to raise awareness of common phishing activities is a physical control that can increase the user's knowledge of phishing, but it may not change their behavior or prevent them from clicking on a link in a phishing message. Implementing email security filters to prevent phishing emails from being delivered is an administrative control that can reduce the exposure to phishing, but it may not be able to block all phishing emails, especially if they are crafted to bypass the filters. Creating additional training for users to recognize the signs of phishing attempts is an administrative control that can improve the user's skills of phishing detection, but it may not guarantee that they will always be vigilant or cautious when receiving an email. Therefore, these options are not the best answer for this question.

Reference = Endpoint Detection and Response – CompTIA Security+ SY0-701 – 2.2, video at 5:30; CompTIA Security+ SY0-701 Certification Study Guide, page 163.

66. Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?
- A. Compensating control
 - B. Network segmentation
 - C. Transfer of risk
 - D. SNMP traps

Answer: A

Explanation:

A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a weakness that cannot be resolved by the primary control. A compensating control does not prevent or eliminate the vulnerability or weakness, but it can reduce the likelihood or impact of an attack. A host-based firewall on a legacy Linux system that allows connections from only specific internal IP addresses is an example of a compensating control, as it can limit the exposure of the system to potential threats from external or unauthorized sources. A host-based firewall is a software application that monitors and filters the incoming and outgoing network traffic on a single host, based on a set of rules or policies. A legacy Linux system is an older version of the Linux operating system that may not be compatible with the latest security updates or patches, and may have known vulnerabilities or weaknesses that could be exploited by attackers.

Reference = Security Controls – SY0-601 CompTIA Security+: 5.1, Security Controls – CompTIA Security+ SY0-501 – 5.7, CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 240. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

67. The management team notices that new accounts that are set up manually do not always have correct access or permissions.

Which of the following automation techniques should a systems administrator use to streamline account creation?

- A. Guard rail script
- B. Ticketing workflow
- C. Escalation script
- D. User provisioning script

Answer: D

Explanation:

A user provisioning script is an automation technique that uses a predefined set of instructions or commands to create, modify, or delete user accounts and assign appropriate access or permissions. A user provisioning script can help to streamline account creation by reducing manual errors, ensuring consistency and compliance, and saving time and resources¹².

The other options are not automation techniques that can streamline account creation:

Guard rail script: This is a script that monitors and enforces the security policies and rules on a system or a network. A guard rail script can help to prevent unauthorized or malicious actions, such as changing security settings, accessing restricted resources, or installing unwanted software³.

Ticketing workflow: This is a process that tracks and manages the requests, issues, or incidents that are reported by users or customers. A ticketing workflow can help to improve the communication, collaboration, and resolution of problems, but it does not automate the account creation process⁴.

Escalation script: This is a script that triggers an alert or a notification when a certain condition or threshold is met or exceeded. An escalation script can help to inform the relevant parties or authorities of a critical situation, such as a security breach, a performance degradation, or a service outage.

Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: User Provisioning – CompTIA Security+ SY0-701 – 5.1, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 1034: CompTIA Security+ SY0-701 Certification Study Guide, page 104.: CompTIA Security+ SY0-701 Certification Study Guide, page 105.

68. A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis.

Which of the following types of controls is the company setting up?

- A. Corrective
- B. Preventive
- C. Detective
- D. Deterrent

Answer: C

Explanation:

A detective control is a type of control that monitors and analyzes the events and activities in a system or

a network, and alerts or reports when an incident or a violation occurs. A SIEM (Security Information and Event Management) system is a tool that collects, correlates, and analyzes the logs from various sources, such as firewalls, routers, servers, or applications, and provides a centralized view of the security status and incidents. An analyst who reviews the logs on a weekly basis can identify and investigate any anomalies, trends, or patterns that indicate a potential threat or a breach. A detective control can help the company to respond quickly and effectively to the incidents, and to improve its security posture and resilience.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 23. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.3, page 14.

69. A systems administrator is looking for a low-cost application-hosting solution that is cloud-based. Which of the following meets these requirements?

- A. Serverless framework
- B. Type 1 hypervisor
- C. SD-WAN
- D. SDN

Answer: A

Explanation:

A serverless framework is a cloud-based application-hosting solution that meets the requirements of low-cost and cloud-based. A serverless framework is a type of cloud computing service that allows developers to run applications without managing or provisioning any servers. The cloud provider handles the server-side infrastructure, such as scaling, load balancing, security, and maintenance, and charges the developer only for the resources consumed by the application. A serverless framework enables developers to focus on the application logic and functionality, and reduces the operational costs and complexity of hosting applications. Some examples of serverless frameworks are AWS Lambda, Azure Functions, and Google Cloud Functions.

A type 1 hypervisor, SD-WAN, and SDN are not cloud-based application-hosting solutions that meet the requirements of low-cost and cloud-based. A type 1 hypervisor is a software layer that runs directly on the hardware and creates multiple virtual machines that can run different operating systems and applications. A type 1 hypervisor is not a cloud-based service, but a virtualization technology that can be used to create private or hybrid clouds. A type 1 hypervisor also requires the developer to manage and provision the servers and the virtual machines, which can increase the operational costs and complexity of hosting applications. Some examples of type 1 hypervisors are VMware ESXi, Microsoft Hyper-V, and Citrix XenServer.

SD-WAN (Software-Defined Wide Area Network) is a network architecture that uses software to dynamically route traffic across multiple WAN connections, such as broadband, LTE, or MPLS. SD-WAN is not a cloud-based service, but a network optimization technology that can improve the performance, reliability, and security of WAN connections. SD-WAN can be used to connect remote sites or users to cloud-based applications, but it does not host the applications itself. Some examples of SD-WAN vendors are Cisco, VMware, and Fortinet.

SDN (Software-Defined Networking) is a network architecture that decouples the control plane from the data plane, and uses a centralized controller to programmatically manage and configure the network devices and traffic flows. SDN is not a cloud-based service, but a network automation technology that can enhance the scalability, flexibility, and efficiency of the network. SDN can be used to create virtual

networks or network functions that can support cloud-based applications, but it does not host the applications itself. Some examples of SDN vendors are OpenFlow, OpenDaylight, and OpenStack. Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 264-265; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 3.1 - Cloud and Virtualization, 7:40 - 10:00; [Serverless Framework]; [Type 1 Hypervisor]; [SD-WAN]; [SDN].

70. A security operations center determines that the malicious activity detected on a server is normal. Which of the following activities describes the act of ignoring detected activity in the future?

- A. Tuning
- B. Aggregating
- C. Quarantining
- D. Archiving

Answer: A

Explanation:

Tuning is the activity of adjusting the configuration or parameters of a security tool or system to optimize its performance and reduce false positives or false negatives. Tuning can help to filter out the normal or benign activity that is detected by the security tool or system, and focus on the malicious or anomalous activity that requires further investigation or response. Tuning can also help to improve the efficiency and effectiveness of the security operations center by reducing the workload and alert fatigue of the analysts. Tuning is different from aggregating, which is the activity of collecting and combining data from multiple sources or sensors to provide a comprehensive view of the security posture. Tuning is also different from quarantining, which is the activity of isolating a potentially infected or compromised device or system from the rest of the network to prevent further damage or spread. Tuning is also different from archiving, which is the activity of storing and preserving historical data or records for future reference or compliance. The act of ignoring detected activity in the future that is deemed normal by the security operations center is an example of tuning, as it involves modifying the settings or rules of the security tool or system to exclude the activity from the detection scope. Therefore, this is the best answer among the given options.

Reference = Security Alerting and Monitoring Concepts and Tools – CompTIA Security+ SY0-701: 4.3, video at 7:00; CompTIA Security+ SY0-701 Certification Study Guide, page 191.

71. A security analyst reviews domain activity logs and notices the following:

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

Which of the following is the best explanation for what the security analyst has discovered?

- A. The user jsmith's account has been locked out.
- B. A keylogger is installed on [smith's workstation
- C. An attacker is attempting to brute force ismith's account.
- D. Ransomware has been deployed in the domain.

Answer: C

Explanation:

Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes – SY0-601 CompTIA Security+: 1.1

72. A company is concerned about weather events causing damage to the server room and downtime. Which of the following should the company consider?

- A. Clustering servers
- B. Geographic dispersion
- C. Load balancers
- D. Off-site backups

Answer: B

Explanation:

Geographic dispersion is a strategy that involves distributing the servers or data centers across different geographic locations. Geographic dispersion can help the company to mitigate the risk of weather events causing damage to the server room and downtime, as well as improve the availability, performance, and resilience of the network. Geographic dispersion can also enhance the disaster recovery and business continuity capabilities of the company, as it can provide backup and failover options in case of a regional outage or disruption¹².

The other options are not the best ways to address the company's concern:

Clustering servers: This is a technique that involves grouping multiple servers together to act as a single system. Clustering servers can help to improve the performance, scalability, and fault tolerance of the network, but it does not protect the servers from physical damage or downtime caused by weather events, especially if the servers are located in the same room or building³.

Load balancers: These are devices or software that distribute the network traffic or workload among multiple servers or resources. Load balancers can help to optimize the utilization, efficiency, and reliability of the network, but they do not prevent the servers from being damaged or disrupted by weather events, especially if the servers are located in the same room or building⁴.

Off-site backups: These are copies of data or files that are stored in a different location than the original source. Off-site backups can help to protect the data from being lost or corrupted by weather events, but they do not prevent the servers from being damaged or disrupted by weather events, nor do they ensure the availability or continuity of the network services.

Reference = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability – CompTIA Security+ SY0-701 – 3.4, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 984: CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

73. Which of the following is a primary security concern for a company setting up a BYOD program?

- A. End of life
- B. Buffer overflow
- C. VM escape
- D. Jailbreaking

Answer: D

Explanation:

Jailbreaking is a primary security concern for a company setting up a BYOD (Bring Your Own Device) program. Jailbreaking is the process of removing the manufacturer's or the carrier's restrictions on a device, such as a smartphone or a tablet, to gain root access and install unauthorized or custom software. Jailbreaking can compromise the security of the device and the data stored on it, as well as expose it to malware, viruses, or hacking. Jailbreaking can also violate the warranty and the terms of service of the device, and make it incompatible with the company's security policies and standards. Therefore, a company setting up a BYOD program should prohibit jailbreaking and enforce device compliance and encryption.

Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 76. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.4, page 11.

74. A company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks.

Which of the following analysis elements did the company most likely use in making this decision?

- A. IMTTR
- B. RTO
- C. ARO
- D. MTBF

Answer: C

Explanation:

ARO (Annualized Rate of Occurrence) is an analysis element that measures the frequency or likelihood of an event happening in a given year. ARO is often used in risk assessment and management, as it helps to estimate the potential loss or impact of an event. A company can use ARO to calculate the annualized loss expectancy (ALE) of an event, which is the product of ARO and the single loss expectancy (SLE). ALE represents the expected cost of an event per year, and can be used to compare with the cost of implementing a security control or purchasing an insurance policy.

The company most likely used ARO in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. The company may have estimated the ARO of ransomware attacks based on historical data, industry trends, or threat intelligence, and found that the ARO was low or negligible. The company may have also calculated the ALE of ransomware attacks, and found that the ALE was lower than the cost of the insurance policy. Therefore, the company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks, as it deemed the risk to be acceptable or manageable.

IMTTR (Incident Management Team Training and Readiness), RTO (Recovery Time Objective), and MTBF (Mean Time Between Failures) are not analysis elements that the company most likely used in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. IMTTR is a process of preparing and training the incident management team to respond effectively to

security incidents. IMTTR does not measure the frequency or impact of an event, but rather the capability and readiness of the team. RTO is a metric that defines the maximum acceptable time for restoring a system or service after a disruption. RTO does not measure the frequency or impact of an event, but rather the availability and continuity of the system or service. MTBF is a metric that measures the average time between failures of a system or component. MTBF does not measure the frequency or impact of an event, but rather the reliability and performance of the system or component.

Reference = CompTIA Security+ SY0-701 Certification Study Guide, page 97-98; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.2 - Risk Management, 0:00 - 3:00.

75. Which of the following is the most likely to be included as an element of communication in a security awareness program?

- A. Reporting phishing attempts or other suspicious activities
- B. Detecting insider threats using anomalous behavior recognition
- C. Verifying information when modifying wire transfer data
- D. Performing social engineering as part of third-party penetration testing

Answer: A

Explanation:

A security awareness program is a set of activities and initiatives that aim to educate and inform the users and employees of an organization about the security policies, procedures, and best practices. A security awareness program can help to reduce the human factor in security risks, such as social engineering, phishing, malware, data breaches, and insider threats. A security awareness program should include various elements of communication, such as newsletters, posters, videos, webinars, quizzes, games, simulations, and feedback mechanisms, to deliver the security messages and reinforce the security culture. One of the most likely elements of communication to be included in a security awareness program is reporting phishing attempts or other suspicious activities, as this can help to raise the awareness of the users and employees about the common types of cyberattacks and how to respond to them. Reporting phishing attempts or other suspicious activities can also help to alert the security team and enable them to take appropriate actions to prevent or mitigate the impact of the attacks. Therefore, this is the best answer among the given options.

The other options are not as likely to be included as elements of communication in a security awareness program, because they are either technical or operational tasks that are not directly related to the security awareness of the users and employees. Detecting insider threats using anomalous behavior recognition is a technical task that involves using security tools or systems to monitor and analyze the activities and behaviors of the users and employees and identify any deviations or anomalies that may indicate malicious or unauthorized actions. This task is usually performed by the security team or the security operations center, and it does not require the communication or participation of the users and employees. Verifying information when modifying wire transfer data is an operational task that involves using verification methods, such as phone calls, emails, or digital signatures, to confirm the authenticity and accuracy of the information related to wire transfers, such as the account number, the amount, or the recipient. This task is usually performed by the financial or accounting department, and it does not involve the security awareness of the users and employees. Performing social engineering as part of third-party penetration testing is a technical task that involves using deception or manipulation techniques, such as phishing, vishing, or impersonation, to test the security posture and the vulnerability of the users and employees to social engineering attacks. This task is usually performed by external

security professionals or consultants, and it does not require the communication or consent of the users and employees. Therefore, these options are not the best answer for this question.

Reference = Security Awareness and Training – CompTIA Security+ SY0-701: 5.2, video at 0:00;
CompTIA Security+ SY0-701 Certification Study Guide, page 263.

76. HOTSPOT

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

INSTRUCTIONS

Not all attacks and remediation actions will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

Answer:


Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

77. HOTSPOT

HOTSPOT

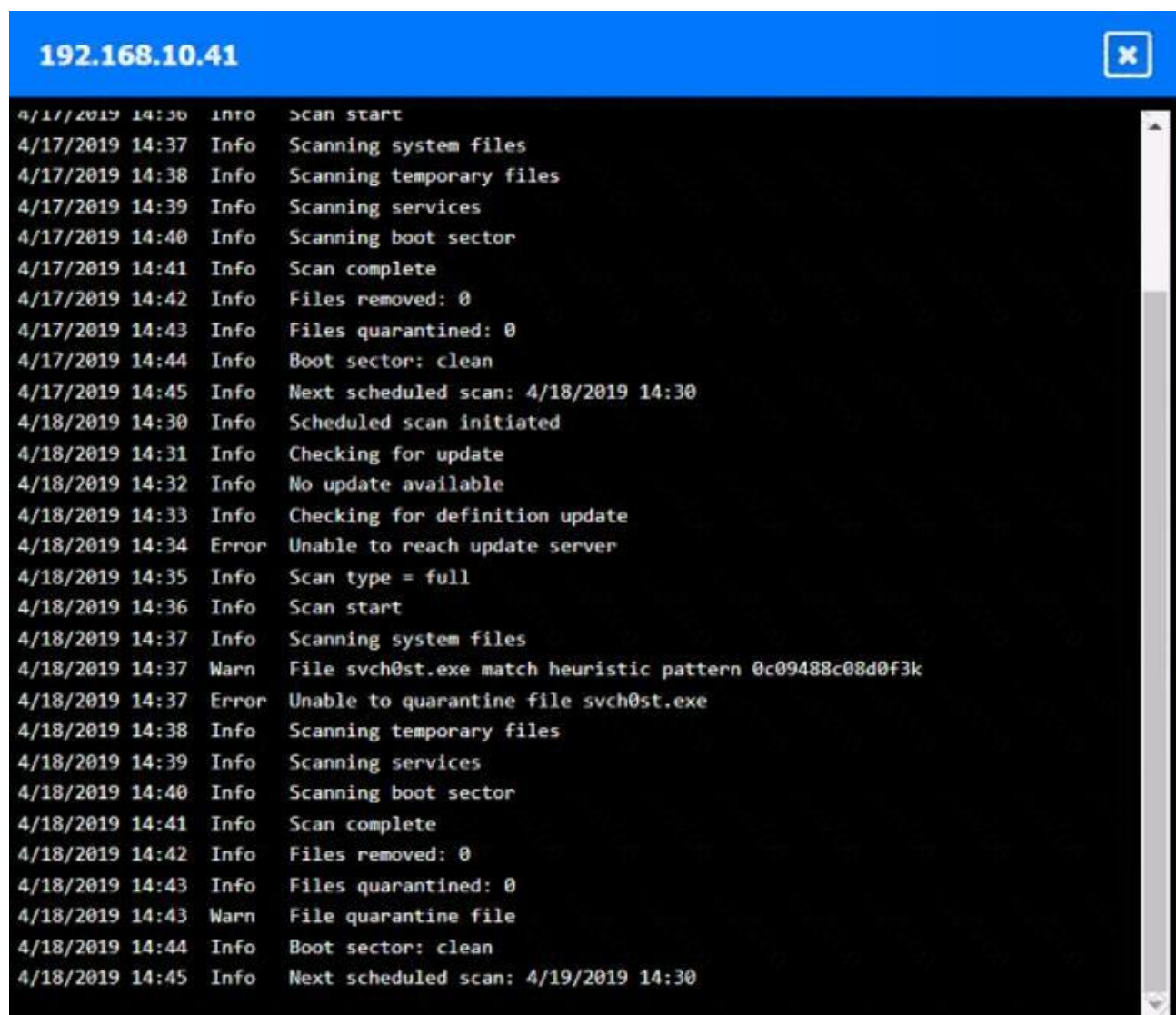
You are security administrator investigating a potential infection on a network.

Click on each host and firewall. Review all logs to determine which host originated the Infection and then deny each remaining hosts clean or infected.

192.168.10.22 

4/17/2019 14:30	Info	Scheduled scan initiated
4/17/2019 14:31	Info	Checking for update
4/17/2019 14:32	Info	No update available
4/17/2019 14:33	Info	Checking for definition update
4/17/2019 14:34	Info	No definition update available
4/17/2019 14:35	Info	Scan type = full
4/17/2019 14:36	Info	Scan start
4/17/2019 14:37	Info	Scanning system files
4/17/2019 14:38	Info	Scanning temporary files
4/17/2019 14:39	Info	Scanning services
4/17/2019 14:40	Info	Scanning boot sector
4/17/2019 14:41	Info	Scan complete
4/17/2019 14:42	Info	Files removed: 0
4/17/2019 14:43	Info	Files quarantined: 0
4/17/2019 14:44	Info	Boot sector: clean
4/17/2019 14:45	Info	Next scheduled scan: 4/18/2019 14:30
4/18/2019 2:31	Warn	Scheduled scan disabled by process svch0st.exe
4/18/2019 2:32	Warn	Scheduled update disabled by process scvh0st.exe

```
192.168.10.37 x
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning complete
```



```
192.168.10.41
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
4/18/2019 14:42 Info Files removed: 0
4/18/2019 14:43 Info Files quarantined: 0
4/18/2019 14:43 Warn File quarantine file
4/18/2019 14:44 Info Boot sector: clean
4/18/2019 14:45 Info Next scheduled scan: 4/19/2019 14:30
```


Firewall



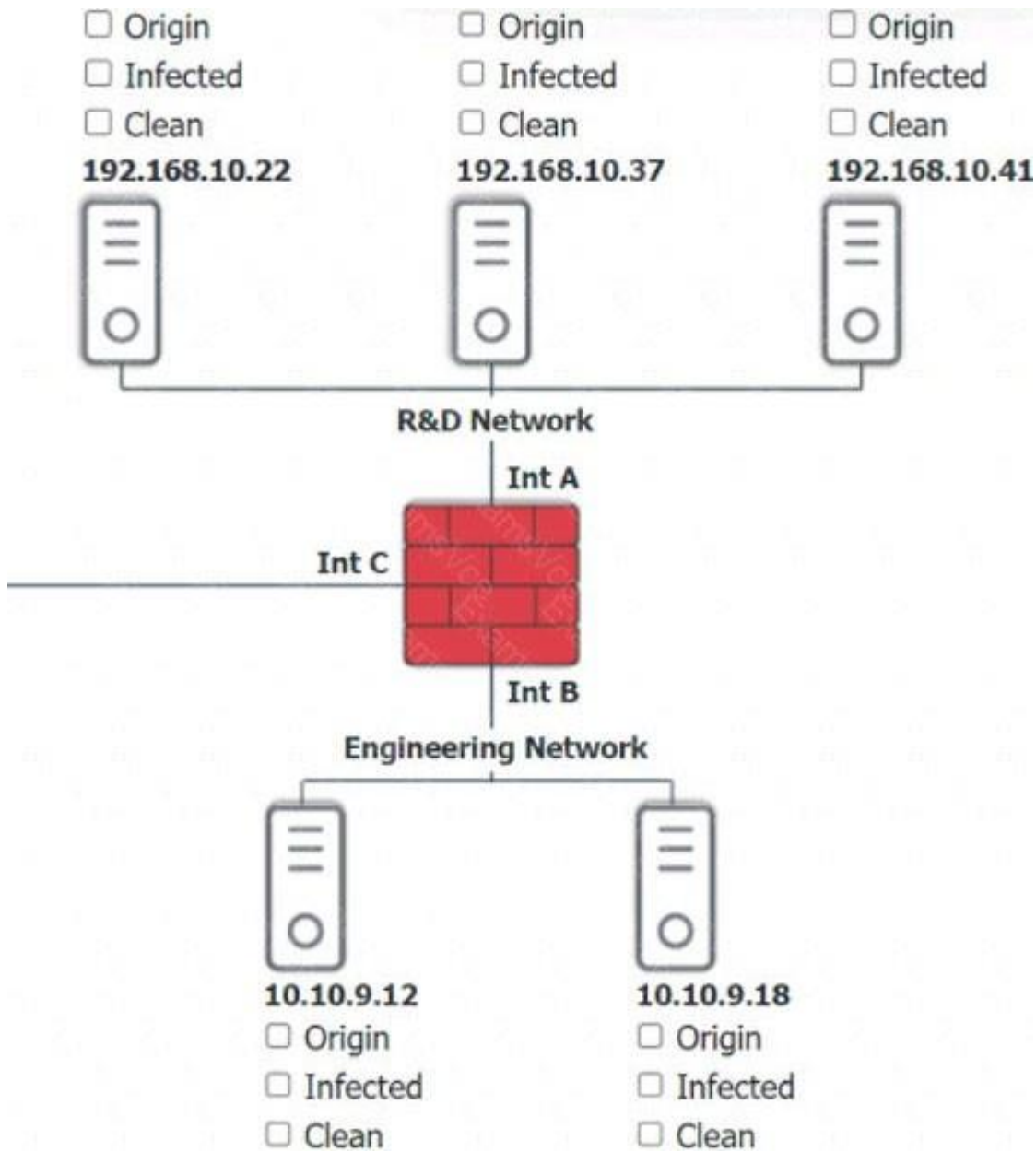
Timestamp	Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019 16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019 16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019 16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504
4/17/2019 16:27:36	192.168.10.41	10.10.9.12	445	smbv1	Permit	345	34757
4/17/2019 16:28:06	10.10.9.12	192.168.10.41	135	rpc	Permit	754	4771
4/17/2019 16:33:31	10.10.9.18	192.168.10.22	135	rpc	Permit	643	2355
4/17/2019 16:35:36	192.168.10.37	10.10.9.12	135	smbv2	Permit	649	5644
4/17/2019 23:58:36	10.10.9.12	192.168.10.41		icmp	Permit	128	128
4/17/2019 23:58:43	10.10.9.12	192.168.10.22		icmp	Permit	128	128
4/17/2019 23:58:45	10.10.9.12	192.168.10.37		icmp	Permit	128	128
4/18/2019 2:31:36	10.10.9.18	192.168.10.41	445	smbv2	Permit	1874	23874
4/18/2019 2:31:45	192.168.10.22	57.203.55.29	8080	http	Permit	7203	75997
4/18/2019 2:31:51	10.10.9.18	57.203.56.201	443	ssl	Permit	9953	199730
4/18/2019 2:31:02	192.168.10.22	57.203.55.234	443	http	Permit	4937	84937
4/18/2019 2:39:11	192.168.10.41	57.203.53.89	8080	http	Permit	8201	133183
4/18/2019 2:39:12	10.10.9.18	57.203.55.19	8080	ssl	Permit	1284	9102854
4/18/2019 2:39:32	192.168.10.37	57.203.56.113	443	ssl	Permit	9341	9938
4/18/2019 13:37:36	192.168.10.22	10.10.9.18	445	smbv3	Permit	1874	23874
4/18/2019 13:39:43	192.168.10.22	10.10.9.18	135	rpc	Permit	673	41358
4/18/2019 13:45:04	10.10.9.18	192.168.10.37	135	rpc	Permit	693	1952
4/18/2019 13:47:44	10.10.9.12	192.168.10.41	445	smbv3	Permit	482	3505
4/18/2019 13:52:57	10.10.9.18	192.168.10.22	135	rpc	Permit	545	9063
4/18/2019 13:53:01	192.168.10.37	10.10.9.12	335	smbv3	Permit	876	8068
4/18/2019 14:30:04	10.10.9.12	57.203.56.231	443	ssl	Permit	9901	199730
4/18/2019 14:30:04	192.168.10.37	57.203.56.143	443	ssl	Permit	10092	209938

10.10.9.12

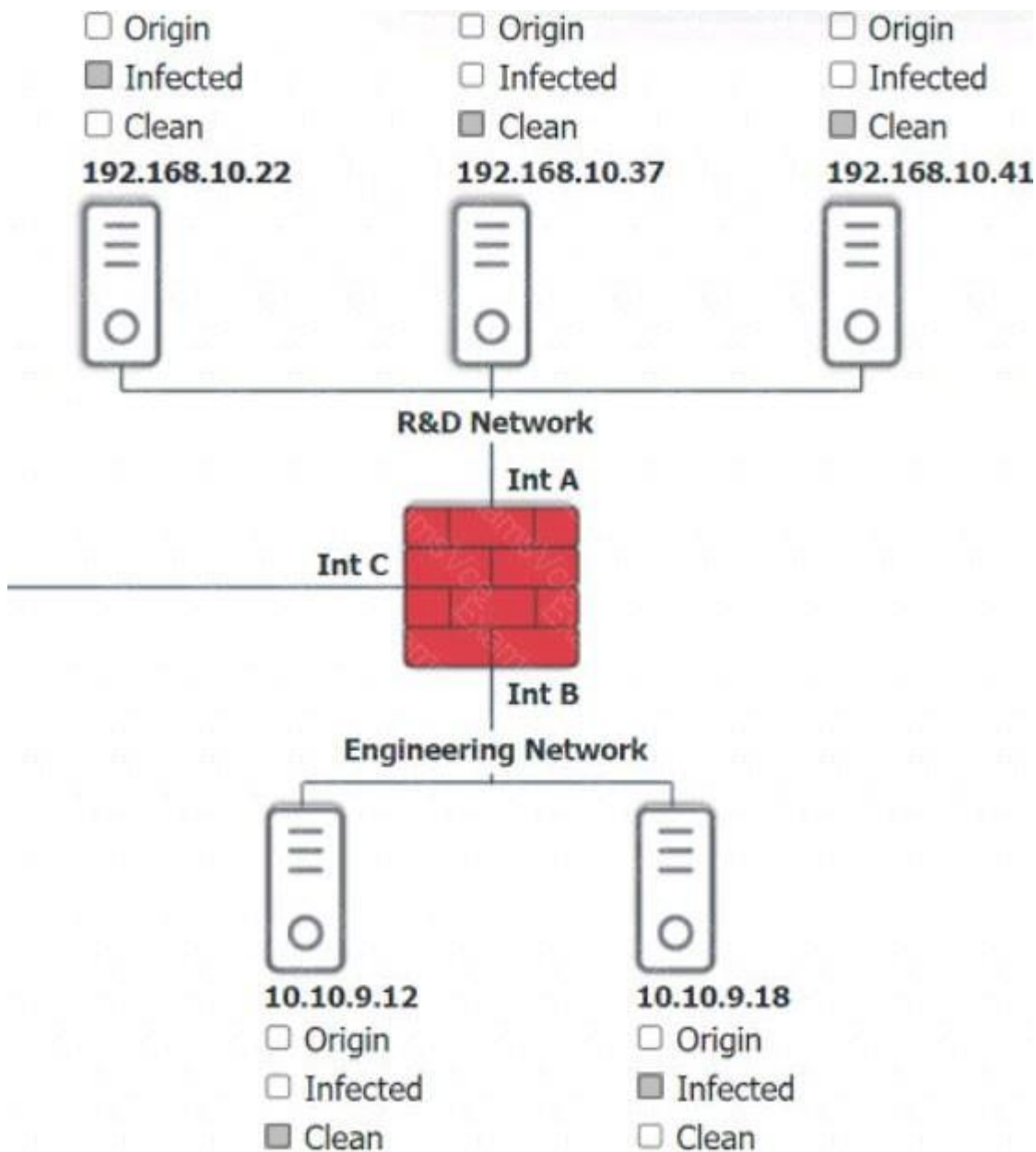
```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Info Update available v10.2.3.4440
4/18/2019 14:33 Info Downloading update
4/18/2019 14:35 Info Definition update complete
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37 Warn File quarantined svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scan complete
```

10.10.9.18

```
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
4/17/2019 14:37 Info Scanning system files
4/17/2019 14:38 Info Scanning temporary files
4/17/2019 14:39 Info Scanning services
4/17/2019 14:40 Info Scanning boot sector
4/17/2019 14:41 Info Scan complete
4/17/2019 14:42 Info Files removed: 0
4/17/2019 14:43 Info Files quarantined: 0
4/17/2019 14:44 Info Boot sector: clean
4/17/2019 14:45 Info Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30 Info Scheduled scan initiated
4/18/2019 14:31 Info Checking for update
4/18/2019 14:32 Info No update available
4/18/2019 14:33 Info Checking for definition update
4/18/2019 14:34 Error Unable to reach update server
4/18/2019 14:35 Info Scan type = full
4/18/2019 14:36 Info Scan start
4/18/2019 14:37 Info Scanning system files
4/18/2019 14:37 Warn File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37 Error Unable to quarantine file svch0st.exe
4/18/2019 14:38 Info Scanning temporary files
4/18/2019 14:39 Info Scanning services
4/18/2019 14:40 Info Scanning boot sector
4/18/2019 14:41 Info Scan complete
```



Answer:

**Explanation:**

Based on the logs, it seems that the host that originated the infection is 192.168.10.22. This host has a suspicious process named `svchost.exe` running on port 443, which is unusual for a Windows service. It also has a large number of outbound connections to different IP addresses on port 443, indicating that it is part of a botnet.

The firewall log shows that this host has been communicating with 10.10.9.18, which is another infected host on the engineering network. This host also has a suspicious process named `svchost.exe` running on port 443, and a large number of outbound connections to different IP addresses on port 443.

The other hosts on the R&D network (192.168.10.37 and 192.168.10.41) are clean, as they do not have any suspicious processes or connections.

78. Which of the following vulnerabilities is exploited when an attacker overwrites a register with a malicious address?

A. VM escape

- B. SQL injection
- C. Buffer overflow
- D. Race condition

Answer: C

Explanation:

A buffer overflow is a vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. A register is a small storage area in the CPU that holds temporary data or instructions. An attacker can exploit a buffer overflow to overwrite a register with a malicious address that points to a shellcode, which is a piece of code that gives the attacker control over the system. By doing so, the attacker can bypass the normal execution flow of the application and execute arbitrary commands.

Reference: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Threats, Attacks, and Vulnerabilities, Section 2.3: Application Attacks, Page 76 1; Buffer Overflows - CompTIA Security+ SY0-701 - 2.3 2

79. Which of the following would be the best way to handle a critical business application that is running on a legacy server?

- A. Segmentation
- B. Isolation
- C. Hardening
- D. Decommissioning

Answer: B

Explanation:

A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats.

One of the best ways to handle a legacy server running a critical business application is to harden it. Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability.

Hardening a legacy server may involve steps such as:

Applying patches and updates to the operating system and the application, if available

Removing or disabling unnecessary services, features, or accounts

Configuring firewall rules and network access control lists to restrict inbound and outbound traffic

Enabling encryption and authentication for data transmission and storage

Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity

Performing regular backups and testing of the system and the application

Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible.

Reference: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 3: Architecture and Design, Section 3.2: Secure System Design, Page 133 1; CompTIA Security+ Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.2: Explain the importance of secure system design, Subobjective: Legacy systems 2

80. Which of the following describes the process of concealing code or text inside a graphical image?

- A. Symmetric encryption
- B. Hashing
- C. Data masking
- D. Steganography

Answer: D

Explanation:

Steganography is the process of hiding information within another medium, such as an image, audio, video, or text file. The hidden information is not visible or noticeable to the casual observer, and can only be extracted by using a specific technique or key. Steganography can be used for various purposes, such as concealing secret messages, watermarking, or evading detection by antivirus software¹²

Reference: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Cryptography and PKI, page 233 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Cryptography and PKI, page 235

81. After a company was compromised, customers initiated a lawsuit. The company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit.

Which of the following describes the action the security team will most likely be required to take?

- A. Retain the emails between the security team and affected customers for 30 days.
- B. Retain any communications related to the security breach until further notice.
- C. Retain any communications between security members during the breach response.
- D. Retain all emails from the company to affected customers for an indefinite period of time.

Answer: B

Explanation:

A legal hold (also known as a litigation hold) is a notification sent from an organization's legal team to employees instructing them not to delete electronically stored information (ESI) or discard paper documents that may be relevant to a new or imminent legal case. A legal hold is intended to preserve evidence and prevent spoliation, which is the intentional or negligent destruction of evidence that could harm a party's case. A legal hold can be triggered by various events, such as a lawsuit, a regulatory investigation, or a subpoena¹²

In this scenario, the company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit filed by the customers after the company was compromised. This means that the security team will most likely be required to retain any communications related to the security breach until further notice. This could include emails, instant messages, reports, logs, memos, or any other documents that could be relevant to the lawsuit. The security team should also inform the relevant custodians (the employees who have access to or control over the ESI) of their preservation obligations and monitor their compliance. The security team should also document the legal hold process and its scope, as well as take steps to protect the ESI from alteration, deletion, or loss³⁴

Reference: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk

Management, page 303 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 305 3: Legal Hold (Litigation Hold) - The Basics of E-Discovery - Exterro 5 4: The Legal Implications and Consequences of a Data Breach 6

82. A network manager wants to protect the company's VPN by implementing multifactor authentication that uses:

- . Something you know
- . Something you have
- . Something you are

Which of the following would accomplish the manager's goal?

- A. Domain name, PKI, GeolIP lookup
- B. VPN IP address, company ID, facial structure
- C. Password, authentication token, thumbprint
- D. Company URL, TLS certificate, home address

Answer: C

Explanation:

The correct answer is C. Password, authentication token, thumbprint. This combination of authentication factors satisfies the manager's goal of implementing multifactor authentication that uses something you know, something you have, and something you are.

Something you know is a type of authentication factor that relies on the user's knowledge of a secret or personal information, such as a password, a PIN, or a security question. A password is a common example of something you know that can be used to access a VPN¹²

Something you have is a type of authentication factor that relies on the user's possession of a physical object or device, such as a smart card, a token, or a smartphone. An authentication token is a common example of something you have that can be used to generate a one-time password (OTP) or a code that can be used to access a VPN¹²

Something you are is a type of authentication factor that relies on the user's biometric characteristics, such as a fingerprint, a face, or an iris. A thumbprint is a common example of something you are that can be used to scan and verify the user's identity to access a VPN¹²

Reference: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Identity and Access Management, page 177 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4: Identity and Access Management, page 179

83. A security manager created new documentation to use in response to various types of security incidents.

Which of the following is the next step the manager should take?

- A. Set the maximum data retention policy.
- B. Securely store the documents on an air-gapped network.
- C. Review the documents' data classification policy.
- D. Conduct a tabletop exercise with the team.

Answer: D

Explanation:

A tabletop exercise is a simulated scenario that tests the effectiveness of a security incident response plan. It involves gathering the relevant stakeholders and walking through the steps of the plan, identifying

any gaps or issues that need to be addressed. A tabletop exercise is a good way to validate the documentation created by the security manager and ensure that the team is prepared for various types of security incidents.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 2841. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 2842.

84. Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked.

Which of the following changes would allow users to access the site?

- A. Creating a firewall rule to allow HTTPS traffic
- B. Configuring the IPS to allow shopping
- C. Tuning the DLP rule that detects credit card data
- D. Updating the categorization in the content filter

Answer: D

Explanation:

A content filter is a device or software that blocks or allows access to web content based on predefined rules or categories. In this case, the new retail website is mistakenly categorized as gambling by the content filter, which prevents users from accessing it. To resolve this issue, the content filter's categorization needs to be updated to reflect the correct category of the website, such as shopping or retail. This will allow the content filter to allow access to the website instead of blocking it.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Technologies and Tools, page 1221. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 3: Technologies and Tools, page 1222.

85. An administrator discovers that some files on a database server were recently encrypted. The administrator sees from the security logs that the data was last accessed by a domain user.

Which of the following best describes the type of attack that occurred?

- A. Insider threat
- B. Social engineering
- C. Watering-hole
- D. Unauthorized attacker

Answer: A

Explanation:

An insider threat is a type of attack that originates from someone who has legitimate access to an organization's network, systems, or data. In this case, the domain user who encrypted the files on the database server is an example of an insider threat, as they abused their access privileges to cause harm to the organization. Insider threats can be motivated by various factors, such as financial gain, revenge, espionage, or sabotage.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 1: General Security Concepts, page 251. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1: General Security Concepts, page 252.

86. Which of the following automation use cases would best enhance the security posture of an

organization by rapidly updating permissions when employees leave a company?

- A. Provisioning resources
- B. Disabling access
- C. Reviewing change approvals
- D. Escalating permission requests

Answer: B

Explanation:

Disabling access is an automation use case that would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company. Disabling access is the process of revoking or suspending the access rights of a user account, such as login credentials, email, VPN, cloud services, etc. Disabling access can prevent unauthorized or malicious use of the account by former employees or attackers who may have compromised the account. Disabling access can also reduce the attack surface and the risk of data breaches or leaks. Disabling access can be automated by using scripts, tools, or workflows that can trigger the action based on predefined events, such as employee termination, resignation, or transfer. Automation can ensure that the access is disabled in a timely, consistent, and efficient manner, without relying on manual intervention or human error.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Identity and Access Management, page 2131. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Identity and Access Management, page 2132.

87. Which of the following must be considered when designing a high-availability network? (Select two).

- A. Ease of recovery
- B. Ability to patch
- C. Physical isolation
- D. Responsiveness
- E. Attack surface
- F. Extensible authentication

Answer: AE

Explanation:

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation of critical services and applications. To achieve this goal, a high-availability network must consider two important factors: ease of recovery and attack surface.

Ease of recovery refers to the ability of a network to quickly restore normal functionality after a failure, disruption, or disaster. A high-availability network should have mechanisms such as redundancy, failover, backup, and restore to ensure that any single point of failure does not cause a complete network outage. A high-availability network should also have procedures and policies for incident response, disaster recovery, and business continuity to minimize the impact of any network issue on the organization's operations and reputation.

Attack surface refers to the exposure of a network to potential threats and vulnerabilities. A high-availability network should have measures such as encryption, authentication, authorization, firewall, intrusion detection and prevention, and patch management to protect the network from unauthorized access, data breaches, malware, denial-of-service attacks, and other cyberattacks. A high-availability network should also have processes and tools for risk assessment, threat intelligence, vulnerability scanning, and penetration testing to identify and mitigate any weaknesses or gaps in the network

security.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Architecture and Design, pages 164-1651. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4: Architecture and Design, pages 164-1652.

88. Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?

- A. Encryption
- B. Hashing
- C. Masking
- D. Tokenization

Answer: C

Explanation:

Masking is a method to secure credit card data that involves replacing some or all of the digits with symbols, such as asterisks, dashes, or Xs, while leaving some of the original digits visible. Masking is best to use when a requirement is to see only the last four numbers on a credit card, as it can prevent unauthorized access to the full card number, while still allowing identification and verification of the cardholder. Masking does not alter the original data, unlike encryption, hashing, or tokenization, which use algorithms to transform the data into different formats.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2: Compliance and Operational Security, page 721. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2: Compliance and Operational Security, page 722.

89. An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk.

Which of the following types of infections is present on the systems?

- A. Virus
- B. Trojan
- C. Spyware
- D. Ransomware

Answer: D

Explanation:

Ransomware is a type of malware that encrypts the victim's files and demands a ransom for the decryption key. The ransomware usually displays a message on the infected system with instructions on how to pay the ransom and recover the files. The .ryk extension is associated with a ransomware variant called Ryuk, which targets large organizations and demands high ransoms¹.

Reference: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 17.

90. A healthcare organization wants to provide a web application that allows individuals to digitally report health emergencies.

Which of the following is the most important consideration during development?

- A. Scalability
- B. Availability
- C. Cost

D. Ease of deployment

Answer: B

Explanation:

Availability is the ability of a system or service to be accessible and usable when needed. For a web application that allows individuals to digitally report health emergencies, availability is the most important consideration during development, because any downtime or delay could have serious consequences for the health and safety of the users. The web application should be designed to handle high traffic, prevent denial-of-service attacks, and have backup and recovery plans in case of failures².

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 41.

91. An organization wants a third-party vendor to do a penetration test that targets a specific device. The organization has provided basic information about the device.

Which of the following best describes this kind of penetration test?

- A. Partially known environment
- B. Unknown environment
- C. Integrated
- D. Known environment

Answer: A

Explanation:

A partially known environment is a type of penetration test where the tester has some information about the target, such as the IP address, the operating system, or the device type. This can help the tester focus on specific vulnerabilities and reduce the scope of the test. A partially known environment is also called a gray box test¹.

Reference: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 10, page 543.

92. An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards.

Which of the following techniques is the attacker using?

- A. Smishing
- B. Disinformation
- C. Impersonating
- D. Whaling

Answer: D

Explanation:

Whaling is a type of phishing attack that targets high-profile individuals, such as executives, celebrities, or politicians. The attacker impersonates someone with authority or influence and tries to trick the victim into performing an action, such as transferring money, revealing sensitive information, or clicking on a malicious link. Whaling is also called CEO fraud or business email compromise².

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 97.

93. An analyst is evaluating the implementation of Zero Trust principles within the data plane.

Which of the following would be most relevant for the analyst to evaluate?

- A. Secured zones
- B. Subject role

- C. Adaptive identity
- D. Threat scope reduction

Answer: A

Explanation:

Secured zones are a key component of the Zero Trust data plane, which is the layer where data is stored, processed, and transmitted. Secured zones are logical or physical segments of the network that isolate data and resources based on their sensitivity and risk. Secured zones enforce granular policies and controls to prevent unauthorized access and lateral movement within the network¹.

Reference: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5, page 255.

94. An organization is leveraging a VPN between its headquarters and a branch location. Which of the following is the VPN protecting?

- A. Data in use
- B. Data in transit
- C. Geographic restrictions
- D. Data sovereignty

Answer: B

Explanation:

Data in transit is data that is moving from one location to another, such as over a network or through the air. Data in transit is vulnerable to interception, modification, or theft by malicious actors. A VPN (virtual private network) is a technology that protects data in transit by creating a secure tunnel between two endpoints and encrypting the data that passes through it².

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, page 145.

95. The marketing department set up its own project management software without telling the appropriate departments.

Which of the following describes this scenario?

- A. Shadow IT
- B. Insider threat
- C. Data exfiltration
- D. Service disruption

Answer: A

Explanation:

Shadow IT is the term used to describe the use of unauthorized or unapproved IT resources within an organization. The marketing department set up its own project management software without telling the appropriate departments, such as IT, security, or compliance. This could pose a risk to the organization's security posture, data integrity, and regulatory compliance¹.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 35.

96. An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be allowed from one device with the IP address 10.50.10.25.

Which of the following firewall ACLs will accomplish this goal?

- A. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53
- Access list outbound deny 10.50.10.25/32 0.0.0.0/0 port 53

B. Access list outbound permit 0.0.0.0/0 10.50.10.25/32 port 53

Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

C. Access list outbound permit 0.0.0.0/0 0.0.0.0/0 port 53

Access list outbound deny 0.0.0.0/0 10.50.10.25/32 port 53

D. Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53

Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

Answer: D

Explanation:

A firewall ACL (access control list) is a set of rules that determines which traffic is allowed or denied by the firewall. The rules are processed in order, from top to bottom, until a match is found.

The syntax of a firewall ACL rule is:

Access list <direction> <action> <source address> <destination address> <protocol> <port>

To limit outbound DNS traffic originating from the internal network, the firewall ACL should allow only the device with the IP address 10.50.10.25 to send DNS requests to any destination on port 53, and deny all other outbound traffic on port 53.

The correct firewall ACL is:

Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53
Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53

The first rule permits outbound traffic from the source address 10.50.10.25/32 (a single host) to any destination address (0.0.0.0/0) on port 53 (DNS). The second rule denies all other outbound traffic on port 532.

Reference: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4, page 175.

97. After a security incident, a systems administrator asks the company to buy a NAC platform.

Which of the following attack surfaces is the systems administrator trying to protect?

A. Bluetooth

B. Wired

C. NFC

D. SCADA

Answer: B

Explanation:

A NAC (network access control) platform is a technology that enforces security policies on devices that attempt to access a network. A NAC platform can verify the identity, role, and compliance of the devices, and grant or deny access based on predefined rules. A NAC platform can protect both wired and wireless networks, but in this scenario, the systems administrator is trying to protect the wired attack surface, which is the set of vulnerabilities that can be exploited through a physical connection to the network¹².

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5, page 189;

CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5, page 237.

98. Which of the following factors are the most important to address when formulating a training curriculum plan for a security awareness program? (Select two).

A. Channels by which the organization communicates with customers

B. The reporting mechanisms for ethics violations

- C. Threat vectors based on the industry in which the organization operates
- D. Secure software development training for all personnel
- E. Cadence and duration of training events
- F. Retraining requirements for individuals who fail phishing simulations

Answer: CE

Explanation:

A training curriculum plan for a security awareness program should address the following factors:

The threat vectors based on the industry in which the organization operates. This will help the employees to understand the specific risks and challenges that their organization faces, and how to protect themselves and the organization from cyberattacks. For example, a healthcare organization may face different threat vectors than a financial organization, such as ransomware, data breaches, or medical device hacking¹.

The cadence and duration of training events. This will help the employees to retain the information and skills they learn, and to keep up with the changing security landscape. The training events should be frequent enough to reinforce the key concepts and behaviors, but not too long or too short to lose the attention or interest of the employees. For example, a security awareness program may include monthly newsletters, quarterly webinars, annual workshops, or periodic quizzes².

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 34; CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2, page 55.

99. An organization disabled unneeded services and placed a firewall in front of a business-critical legacy system.

Which of the following best describes the actions taken by the organization?

- A. Exception
- B. Segmentation
- C. Risk transfer
- D. Compensating controls

Answer: D

Explanation:

Compensating controls are alternative security measures that are implemented when the primary controls are not feasible, cost-effective, or sufficient to mitigate the risk. In this case, the organization used compensating controls to protect the legacy system from potential attacks by disabling unneeded services and placing a firewall in front of it. This reduced the attack surface and the likelihood of exploitation.

Reference: Official CompTIA Security+ Study Guide (SY0-701), page 29

Security Controls - CompTIA Security+ SY0-701 - 1.1 1

100. Which of the following is the best reason to complete an audit in a banking environment?

- A. Regulatory requirement
- B. Organizational change
- C. Self-assessment requirement
- D. Service-level requirement

Answer: A

Explanation:

A regulatory requirement is a mandate imposed by a government or an authority that must be followed by an organization or an individual. In a banking environment, audits are often required by regulators to ensure compliance with laws, standards, and policies related to security, privacy, and financial reporting. Audits help to identify and correct any gaps or weaknesses in the security posture and the internal controls of the organization.

Reference: Official CompTIA Security+ Study Guide (SY0-701), page 507
Security+ (Plus) Certification | CompTIA IT Certifications 2

101. A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data.

Which of the following should the administrator do first?

- A. Block access to cloud storage websites.
- B. Create a rule to block outgoing email attachments.
- C. Apply classifications to the data.
- D. Remove all user permissions from shares on the file server.

Answer: C

Explanation:

Data classification is the process of assigning labels or tags to data based on its sensitivity, value, and risk. Data classification is the first step in a data loss prevention (DLP) solution, as it helps to identify what data needs to be protected and how. By applying classifications to the data, the security administrator can define appropriate policies and rules for the DLP solution to prevent the exfiltration of sensitive customer data.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Data Protection, page 323. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 8: Data Protection, page 327.

102. Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

- A. SIEM
- B. DLP
- C. IDS
- D. SNMP

Answer: A

Explanation:

SIEM stands for Security Information and Event Management. It is a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system. SIEM can analyze the collected data, correlate events, generate alerts, and provide reports and dashboards. SIEM can also integrate with other security tools and support compliance requirements. SIEM helps organizations to detect and respond to cyber threats, improve security posture, and reduce operational costs.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Monitoring and Auditing, page 393. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 10: Monitoring and Auditing, page 397.

103. Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).

- A. The device has been moved from a production environment to a test environment.
- B. The device is configured to use cleartext passwords.
- C. The device is moved to an isolated segment on the enterprise network.
- D. The device is moved to a different location in the enterprise.
- E. The device's encryption level cannot meet organizational standards.
- F. The device is unable to receive authorized updates.

Answer: E

Explanation:

An engineer should recommend the decommissioning of a network device when the device poses a security risk or a compliance violation to the enterprise environment. A device that cannot meet the encryption standards or receive authorized updates is vulnerable to attacks and breaches, and may expose sensitive data or compromise network integrity. Therefore, such a device should be removed from the network and replaced with a more secure and updated one.

Reference

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, Section 2.2, page 671

CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 2, Question 16, page 512

104. An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period.

Which of the following data policies is the administrator carrying out?

- A. Compromise
- B. Retention
- C. Analysis
- D. Transfer
- E. Inventory

Answer: B

Explanation:

A data retention policy is a set of rules that defines how long data should be stored and when it should be deleted or archived. An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period by following the data retention policy of the organization. This policy helps the organization to comply with legal and regulatory requirements, optimize storage space, and protect data privacy and security.

Reference

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, Section 3.4, page 1211

CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 3, Question 15, page 832

105. A systems administrator is working on a solution with the following requirements:

- Provide a secure zone.
- Enforce a company-wide access control policy.
- Reduce the scope of threats.

Which of the following is the systems administrator setting up?

- A. Zero Trust

- B. AAA
- C. Non-repudiation
- D. CIA

Answer: A

Explanation:

Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company-wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.

Reference: 5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models.

8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices.

106. A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes.

Which of the following should the administrator set up to achieve this goal?

- A. SPF
- B. GPO
- C. NAC
- D. FIM

Answer: D

Explanation:

FIM stands for File Integrity Monitoring, which is a method to secure data by detecting any changes or modifications to files, directories, or registry keys. FIM can help a security administrator track any unauthorized or malicious changes to the data, as well as verify the integrity and compliance of the data. FIM can also alert the administrator of any potential breaches or incidents involving the data.

Some of the benefits of FIM are:

It can prevent data tampering and corruption by verifying the checksums or hashes of the files.

It can identify the source and time of the changes by logging the user and system actions.

It can enforce security policies and standards by comparing the current state of the data with the baseline or expected state.

It can support forensic analysis and incident response by providing evidence and audit trails of the changes.

Reference: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 5: Technologies and Tools, Section 5.3:

Security Tools, p. 209-210

CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 2: Technologies and Tools,

Objective 2.4: Given a scenario, analyze and interpret output from security technologies, Sub-objective:

File integrity monitor, p. 12

107. Which of the following is the phase in the incident response process when a security analyst reviews

roles and responsibilities?

- A. Preparation
- B. Recovery
- C. Lessons learned
- D. Analysis

Answer: A

Explanation:

Preparation is the phase in the incident response process when a security analyst reviews roles and responsibilities, as well as the policies and procedures for handling incidents. Preparation also involves gathering and maintaining the necessary tools, resources, and contacts for responding to incidents. Preparation can help a security analyst to be ready and proactive when an incident occurs, as well as to reduce the impact and duration of the incident.

Some of the activities that a security analyst performs during the preparation phase are:

Defining the roles and responsibilities of the incident response team members, such as the incident manager, the incident coordinator, the technical lead, the communications lead, and the legal advisor. Establishing the incident response plan, which outlines the objectives, scope, authority, and procedures for responding to incidents, as well as the escalation and reporting mechanisms.

Developing the incident response policy, which defines the types and categories of incidents, the severity levels, the notification and reporting requirements, and the roles and responsibilities of the stakeholders.

Creating the incident response playbook, which provides the step-by-step guidance and checklists for handling specific types of incidents, such as denial-of-service, ransomware, phishing, or data breach.

Acquiring and testing the incident response tools, such as network and host-based scanners, malware analysis tools, forensic tools, backup and recovery tools, and communication and collaboration tools.

Identifying and securing the incident response resources, such as the incident response team, the incident response location, the evidence storage, and the external support.

Building and maintaining the incident response contacts, such as the internal and external stakeholders, the law enforcement agencies, the regulatory bodies, and the media.

Reference: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 6: Architecture and Design, Section 6.4: Secure Systems Design, p. 279-280

CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 3: Architecture and Design, Objective 3.5: Given a scenario, implement secure network architecture concepts, Sub-objective: Incident response, p. 16

108. A company is discarding a classified storage array and hires an outside vendor to complete the disposal.

Which of the following should the company request from the vendor?

- A. Certification
- B. Inventory list
- C. Classification
- D. Proof of ownership

Answer: A

Explanation:

The company should request a certification from the vendor that confirms the storage array has been disposed of securely and in compliance with the company's policies and standards. A certification

provides evidence that the vendor has followed the proper procedures and methods to destroy the classified data and prevent unauthorized access or recovery. A certification may also include details such as the date, time, location, and method of disposal, as well as the names and signatures of the personnel involved.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 1441

109. Which of the following would be the best ways to ensure only authorized personnel can access a secure facility? (Select two).

- A. Fencing
- B. Video surveillance
- C. Badge access
- D. Access control vestibule
- E. Sign-in sheet
- F. Sensor

Answer: CD

Explanation:

Badge access and access control vestibule are two of the best ways to ensure only authorized personnel can access a secure facility. Badge access requires the personnel to present a valid and authenticated badge to a reader or scanner that grants or denies access based on predefined rules and permissions. Access control vestibule is a physical security measure that consists of a small room or chamber with two doors, one leading to the outside and one leading to the secure area. The personnel must enter the vestibule and wait for the first door to close and lock before the second door can be opened. This prevents tailgating or piggybacking by unauthorized individuals.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, pages 197-1981

110. A company's marketing department collects, modifies, and stores sensitive customer data. The infrastructure team is responsible for securing the data while in transit and at rest.

Which of the following data roles describes the customer?

- A. Processor
- B. Custodian
- C. Subject
- D. Owner

Answer: C

Explanation:

According to the CompTIA Security+ SY0-701 Certification Study Guide, data subjects are the individuals whose personal data is collected, processed, or stored by an organization. Data subjects have certain rights and expectations regarding how their data is handled, such as the right to access, correct, delete, or restrict their data. Data subjects are different from data owners, who are the individuals or entities that have the authority and responsibility to determine how data is classified, protected, and used. Data subjects are also different from data processors, who are the individuals or entities that perform operations on data on behalf of the data owner, such as collecting, modifying, storing, or transmitting data. Data subjects are also different from data custodians, who are the individuals or entities that implement the security controls and procedures specified by the data owner to protect data while in transit and at rest.

Reference

CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Data Security, page 511

111. Malware spread across a company's network after an employee visited a compromised industry blog.

Which of the following best describes this type of attack?

- A. Impersonation
- B. Disinformation
- C. Watering-hole
- D. Smishing

Answer: C

Explanation:

A watering-hole attack is a type of cyberattack that targets groups of users by infecting websites that they commonly visit. The attackers exploit vulnerabilities to deliver a malicious payload to the organization's network. The attack aims to infect users' computers and gain access to a connected corporate network. The attackers target websites known to be popular among members of a particular organization or demographic. The attack differs from phishing and spear-phishing attacks, which typically attempt to steal data or install malware onto users' devices¹

In this scenario, the compromised industry blog is the watering hole that the attackers used to spread malware across the company's network. The attackers likely chose this blog because they knew that the employees of the company were interested in its content and visited it frequently. The attackers may have injected malicious code into the blog or redirected the visitors to a spoofed website that hosted the malware. The malware then infected the employees' computers and propagated to the network.

Reference

1: Watering Hole Attacks: Stages, Examples, Risk Factors & Defense ...

112. After a recent ransomware attack on a company's system, an administrator reviewed the log files.

Which of the following control types did the administrator use?

- A. Compensating
- B. Detective
- C. Preventive
- D. Corrective

Answer: B

Explanation:

Detective controls are security measures that are designed to identify and monitor any malicious activity or anomalies on a system or network. They can help to discover the source, scope, and impact of an attack, and provide evidence for further analysis or investigation. Detective controls include log files, security audits, intrusion detection systems, network monitoring tools, and antivirus software. In this case, the administrator used log files as a detective control to review the ransomware attack on the company's system. Log files are records of events and activities that occur on a system or network, such as user actions, system errors, network traffic, and security alerts. They can provide valuable information for troubleshooting, auditing, and forensics.

Reference: Security+ (Plus) Certification | CompTIA IT Certifications, under "About the exam", bullet point 3: "Operate with an awareness of applicable regulations and policies, including principles of

governance, risk, and compliance.”

CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 14: “Detective controls are designed to identify and monitor any malicious activity or anomalies on a system or network.”

Control Types – CompTIA Security+ SY0-401: 2.1 - Professor Messer IT ..., under “Detective Controls”: “Detective controls are security measures that are designed to identify and monitor any malicious activity or anomalies on a system or network.”

113. Which of the following agreement types defines the time frame in which a vendor needs to respond?

- A. SOW
- B. SLA
- C. MOA
- D. MOU

Answer: B

Explanation:

A service level agreement (SLA) is a type of agreement that defines the expectations and responsibilities between a service provider and a customer. It usually includes the quality, availability, and performance metrics of the service, as well as the time frame in which the provider needs to respond to service requests, incidents, or complaints. An SLA can help ensure that the customer receives the desired level of service and that the provider is accountable for meeting the agreed-upon standards.

Reference: Security+ (Plus) Certification | CompTIA IT Certifications, under “About the exam”, bullet point 3: “Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.”

CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 14: “Service Level Agreements (SLAs) are contracts between a service provider and a customer that specify the level of service expected from the service provider.”

114. A Chief Information Security Officer wants to monitor the company's servers for SQLi attacks and allow for comprehensive investigations if an attack occurs. The company uses SSL decryption to allow traffic monitoring.

Which of the following strategies would best accomplish this goal?

- A. Logging all NetFlow traffic into a SIEM
- B. Deploying network traffic sensors on the same subnet as the servers
- C. Logging endpoint and OS-specific security logs
- D. Enabling full packet capture for traffic entering and exiting the servers

Answer: D

Explanation:

Full packet capture is a technique that records all network traffic passing through a device, such as a router or firewall. It allows for detailed analysis and investigation of network events, such as SQLi attacks, by providing the complete content and context of the packets. Full packet capture can help identify the source, destination, payload, and timing of an SQLi attack, as well as the impact on the server and database. Logging NetFlow traffic, network traffic sensors, and endpoint and OS-specific security logs can provide some information about network activity, but they do not capture the full content of the packets, which may limit the scope and depth of the investigation.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 372-373

115. A client demands at least 99.99% uptime from a service provider's hosted security services. Which of the following documents includes the information the service provider should return to the client?

- A. MOA
- B. SOW
- C. MOU
- D. SLA

Answer: D

Explanation:

A service level agreement (SLA) is a document that defines the level of service expected by a customer from a service provider, indicating the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved. An SLA can specify the minimum uptime or availability of a service, such as 99.99%, and the consequences for failing to meet that standard. A memorandum of agreement (MOA), a statement of work (SOW), and a memorandum of understanding (MOU) are other types of documents that can be used to establish a relationship between parties, but they do not typically include the details of service levels and performance metrics that an SLA does.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17

116. A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices.

Which of the following vulnerabilities is the organization addressing?

- A. Cross-site scripting
- B. Buffer overflow
- C. Jailbreaking
- D. Side loading

Answer: C

Explanation:

Jailbreaking is the process of removing the restrictions imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking allows users to install unauthorized applications, modify system settings, and access root privileges. However, jailbreaking also exposes the device to potential security risks, such as malware, spyware, unauthorized access, data loss, and voided warranty. Therefore, an organization may prohibit employees from jailbreaking their mobile devices to prevent these vulnerabilities and protect the corporate data and network.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 507 2

117. Which of the following practices would be best to prevent an insider from introducing malicious code into a company's development process?

- A. Code scanning for vulnerabilities
- B. Open-source component usage
- C. Quality assurance testing
- D. Peer review and approval

Answer: D

Explanation:

Peer review and approval is a practice that involves having other developers or experts review the code before it is deployed or released. Peer review and approval can help detect and prevent malicious code, errors, bugs, vulnerabilities, and poor quality in the development process. Peer review and approval can also enforce coding standards, best practices, and compliance requirements. Peer review and approval can be done manually or with the help of tools, such as code analysis, code review, and code signing.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 543 2

118. A systems administrator is creating a script that would save time and prevent human error when performing account creation for a large number of end users.

Which of the following would be a good use case for this task?

- A. Off-the-shelf software
- B. Orchestration
- C. Baseline
- D. Policy enforcement

Answer: B

Explanation:

Orchestration is the process of automating multiple tasks across different systems and applications. It can help save time and reduce human error by executing predefined workflows and scripts. In this case, the systems administrator can use orchestration to create accounts for a large number of end users without having to manually enter their information and assign permissions.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 457 1

119. After an audit, an administrator discovers all users have access to confidential data on a file server.

Which of the following should the administrator use to restrict access to the data quickly?

- A. Group Policy
- B. Content filtering
- C. Data loss prevention
- D. Access control lists

Answer: D

Explanation:

Access control lists (ACLs) are rules that specify which users or groups can access which resources on a file server. They can help restrict access to confidential data by granting or denying permissions based on the identity or role of the user. In this case, the administrator can use ACLs to quickly modify the access rights of the users and prevent them from accessing the data they are not authorized to see.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308 1

120. A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team.

Which of the following best describes the threat actor in the CISO's report?

- A. Insider threat
- B. Hacktivist

- C. Nation-state
- D. Organized crime

Answer: D

Explanation:

Ransomware-as-a-service is a type of cybercrime where hackers sell or rent ransomware tools or services to other criminals who use them to launch attacks and extort money from victims. This is a typical example of organized crime, which is a group of criminals who work together to conduct illegal activities for profit. Organized crime is different from other types of threat actors, such as insider threats, hacktivists, or nation-states, who may have different motives, methods, or targets.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17 1

121. A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

- A. Patch availability
- B. Product software compatibility
- C. Ease of recovery
- D. Cost of replacement

Answer: A

Explanation:

End-of-life operating systems are those that are no longer supported by the vendor or manufacturer, meaning they do not receive any security updates or patches. This makes them vulnerable to exploits and attacks that take advantage of known or unknown flaws in the software. Patch availability is the security implication of using end-of-life operating systems, as it affects the ability to fix or prevent security issues. Other factors, such as product software compatibility, ease of recovery, or cost of replacement, are not directly related to security, but rather to functionality, availability, or budget.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 29 1

122. A company is developing a critical system for the government and storing project information on a fileshare.

Which of the following describes how this data will most likely be classified? (Select two).

- A. Private
- B. Confidential
- C. Public
- D. Operational
- E. Urgent
- F. Restricted

Answer: BF

Explanation:

Data classification is the process of assigning labels to data based on its sensitivity and business impact. Different organizations and sectors may have different data classification schemes, but a common one is the following¹:

Public: Data that can be freely disclosed to anyone without any harm or risk.

Private: Data that is intended for internal use only and may cause some harm or risk if disclosed.

Confidential: Data that is intended for authorized use only and may cause significant harm or risk if disclosed.

Restricted: Data that is intended for very limited use only and may cause severe harm or risk if disclosed.

In this scenario, the company is developing a critical system for the government and storing project information on a fileshare. This data is likely to be classified as confidential and restricted, because it is not meant for public or private use, and it may cause serious damage to national security or public safety if disclosed. The government may also have specific requirements or regulations for handling such data, such as encryption, access control, and auditing².

Reference: 1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17 2: Data Classification Practices: Final Project Description Released

123. After reviewing the following vulnerability scanning report:

Server:192.168.14.6

Service: Telnet

Port: 23 Protocol: TCP

Status: Open Severity: High

Vulnerability: Use of an insecure network protocol

A security analyst performs the following test:

```
nmap -p 23 192.168.14.6 --script telnet-encryption
```

PORT STATE SERVICE REASON

23/tcp open telnet syn-ack

I telnet encryption:

```
|_ Telnet server supports encryption
```

Which of the following would the security analyst conclude for this reported vulnerability?

- A. It is a false positive.
- B. A rescan is required.
- C. It is considered noise.
- D. Compensating controls exist.

Answer: A

Explanation:

A false positive is a result that indicates a vulnerability or a problem when there is none. In this case, the vulnerability scanning report shows that the telnet service on port 23 is open and uses an insecure network protocol. However, the security analyst performs a test using nmap and a script that checks for telnet encryption support. The result shows that the telnet server supports encryption, which means that the data transmitted between the client and the server can be protected from eavesdropping. Therefore, the reported vulnerability is a false positive and does not reflect the actual security posture of the server. The security analyst should verify the encryption settings of the telnet server and client and ensure that they are configured properly³.

Reference: 3: Telnet Protocol - Can You Encrypt Telnet?

124. A security consultant needs secure, remote access to a client environment.

Which of the following should the security consultant most likely use to gain access?

- A. EAP

- B. DHCP
- C. IPSec
- D. NAT

Answer: C

Explanation:

IPSec is a protocol suite that provides secure communication over IP networks. IPSec can be used to create virtual private networks (VPNs) that encrypt and authenticate the data exchanged between two or more parties. IPSec can also provide data integrity, confidentiality, replay protection, and access control. A security consultant can use IPSec to gain secure, remote access to a client environment by establishing a VPN tunnel with the client's network.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 385 1

125. Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

- A. Impact analysis
- B. Scheduled downtime
- C. Backout plan
- D. Change management boards

Answer: B

Explanation:

Scheduled downtime is a planned period of time when a system or service is unavailable for maintenance, updates, upgrades, or other changes. Scheduled downtime gives administrators a set period to perform changes to an operational system without disrupting the normal business operations or affecting the availability of the system or service. Scheduled downtime also allows administrators to inform the users and stakeholders about the expected duration and impact of the changes.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 579 1

126. Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

- A. Configure all systems to log scheduled tasks.
- B. Collect and monitor all traffic exiting the network.
- C. Block traffic based on known malicious signatures.
- D. Install endpoint management software on all systems.

Answer: D

Explanation:

Endpoint management software is a tool that allows security engineers to monitor and control the configuration, security, and performance of workstations and servers from a central console. Endpoint management software can help detect and prevent unauthorized changes and software installations, enforce policies and compliance, and provide reports and alerts on the status of the endpoints. The other options are not as effective or comprehensive as endpoint management software for this purpose.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 137 1

127. After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice.

Which of the following topics did the user recognize from the training?

- A. Insider threat
- B. Email phishing
- C. Social engineering
- D. Executive whaling

Answer: C

Explanation:

Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment. The user recognized this as a potential scam and reported it to the IT help desk. The other topics are not relevant to this situation.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 19 1

128. Which of the following exercises should an organization use to improve its incident response process?

- A. Tabletop
- B. Replication
- C. Failover
- D. Recovery

Answer: A

Explanation:

A tabletop exercise is a simulated scenario that tests the organization's incident response plan and procedures. It involves key stakeholders and decision-makers who discuss their roles and actions in response to a hypothetical incident. It can help identify gaps, weaknesses, and improvement areas in the incident response process. It can also enhance communication, coordination, and collaboration among the participants.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 525 1

129. Which of the following is used to validate a certificate when it is presented to a user?

- A. OCSP
- B. CSR
- C. CA
- D. CRC

Answer: A

Explanation:

OCSP stands for Online Certificate Status Protocol. It is a protocol that allows applications to check the revocation status of a certificate in real-time. It works by sending a query to an OCSP responder, which is a server that maintains a database of revoked certificates. The OCSP responder returns a response that indicates whether the certificate is valid, revoked, or unknown. OCSP is faster and more efficient than downloading and parsing Certificate Revocation Lists (CRLs), which are large files that contain the

serial numbers of all revoked certificates issued by a Certificate Authority (CA).

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 337 1

130. A newly identified network access vulnerability has been found in the OS of legacy IoT devices. Which of the following would best mitigate this vulnerability quickly?

- A. Insurance
- B. Patching
- C. Segmentation
- D. Replacement

Answer: C

Explanation:

Segmentation is a technique that divides a network into smaller subnetworks or segments, each with its own security policies and controls. Segmentation can help mitigate network access vulnerabilities in legacy IoT devices by isolating them from other devices and systems, reducing their attack surface and limiting the potential impact of a breach. Segmentation can also improve network performance and efficiency by reducing congestion and traffic. Patching, insurance, and replacement are other possible strategies to deal with network access vulnerabilities, but they may not be feasible or effective in the short term. Patching may not be available or compatible for legacy IoT devices, insurance may not cover the costs or damages of a cyberattack, and replacement may be expensive and time-consuming.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143

131. A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

- A. Encryption at rest
- B. Masking
- C. Data classification
- D. Permission restrictions

Answer: A

Explanation:

Encryption at rest is a strategy that protects data stored on a device, such as a laptop, by converting it into an unreadable format that can only be accessed with a decryption key or password. Encryption at rest can prevent data loss on stolen laptops by preventing unauthorized access to the data, even if the device is physically compromised. Encryption at rest can also help comply with data privacy regulations and standards that require data protection. Masking, data classification, and permission restrictions are other strategies that can help protect data, but they may not be sufficient or applicable for data stored on laptops. Masking is a technique that obscures sensitive data elements, such as credit card numbers, with random characters or symbols, but it is usually used for data in transit or in use, not at rest. Data classification is a process that assigns labels to data based on its sensitivity and business impact, but it does not protect the data itself. Permission restrictions are rules that define who can access, modify, or delete data, but they may not prevent unauthorized access if the laptop is stolen and the security controls are bypassed.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17-18, 372-373

132.Which of the following would be best suited for constantly changing environments?

- A. RTOS
- B. Containers
- C. Embedded systems
- D. SCADA

Answer: B

Explanation:

Containers are a method of virtualization that allows applications to run in isolated environments with their own dependencies, libraries, and configurations. Containers are best suited for constantly changing environments because they are lightweight, portable, scalable, and easy to deploy and update. Containers can also support microservices architectures, which enable faster and more frequent delivery of software features.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 512 1

133.A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network.

Which of the following changes should the security analyst recommend?

- A. Changing the remote desktop port to a non-standard number
- B. Setting up a VPN and placing the jump server inside the firewall
- C. Using a proxy for web connections from the remote desktop server
- D. Connecting the remote server to the domain and increasing the password length

Answer: B

Explanation:

A VPN is a virtual private network that creates a secure tunnel between two or more devices over a public network. A VPN can encrypt and authenticate the data, as well as hide the IP addresses and locations of the devices. A jump server is a server that acts as an intermediary between a user and a target server, such as a production server. A jump server can provide an additional layer of security and access control, as well as logging and auditing capabilities. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can protect the internal network from external threats and limit the exposure of sensitive services and ports. A security analyst should recommend setting up a VPN and placing the jump server inside the firewall to improve the security of the remote desktop access to the production network. This way, the remote desktop service will not be exposed to the public network, and only authorized users with VPN credentials can access the jump server and then the production server.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 382-383 1; Chapter 9: Network Security, page 441-442 1

134. Which of the following involves an attempt to take advantage of database misconfigurations?

- A. Buffer overflow
- B. SQL injection
- C. VM escape
- D. Memory injection

Answer: B

Explanation:

SQL injection is a type of attack that exploits a database misconfiguration or a flaw in the application code that interacts with the database. An attacker can inject malicious SQL statements into the user input fields or the URL parameters that are sent to the database server. These statements can then execute unauthorized commands, such as reading, modifying, deleting, or creating data, or even taking over the database server. SQL injection can compromise the confidentiality, integrity, and availability of the data and the system.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215 1

135. An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network.

Which of the following should the administrator use to accomplish this goal?

- A. Segmentation
- B. Isolation
- C. Patching
- D. Encryption

Answer: A

Explanation:

Segmentation is a network design technique that divides the network into smaller and isolated segments based on logical or physical boundaries. Segmentation can help improve network security by limiting the scope of an attack, reducing the attack surface, and enforcing access control policies. Segmentation can also enhance network performance, scalability, and manageability. To accomplish the goal of storing customer data on a separate part of the network, the administrator can use segmentation technologies such as subnetting, VLANs, firewalls, routers, or switches.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 1

136. Which of the following is used to quantitatively measure the criticality of a vulnerability?

- A. CVE
- B. CVSS
- C. CIA
- D. CERT

Answer: B

Explanation:

CVSS stands for Common Vulnerability Scoring System, which is a framework that provides a standardized way to assess and communicate the severity and risk of vulnerabilities. CVSS uses a set of metrics and formulas to calculate a numerical score ranging from 0 to 10, where higher scores indicate higher criticality. CVSS can help organizations prioritize remediation efforts and compare vulnerabilities across different systems and vendors. The other options are not used to measure the criticality of a vulnerability, but rather to identify, classify, or report them.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 39

137. A technician is opening ports on a firewall for a new system being deployed and supported by a SaaS provider.

Which of the following is a risk in the new system?

- A. Default credentials

- B. Non-segmented network
- C. Supply chain vendor
- D. Vulnerable software

Answer: C

Explanation:

A supply chain vendor is a third-party entity that provides goods or services to an organization, such as a SaaS provider. A supply chain vendor can pose a risk to the new system if the vendor has poor security practices, breaches, or compromises that could affect the confidentiality, integrity, or availability of the system or its data. The organization should perform due diligence and establish a service level agreement with the vendor to mitigate this risk. The other options are not specific to the scenario of using a SaaS provider, but rather general risks that could apply to any system.

138. Which of the following security concepts is the best reason for permissions on a human resources fileshare to follow the principle of least privilege?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Non-repudiation

Answer: C

Explanation:

Confidentiality is the security concept that ensures data is protected from unauthorized access or disclosure. The principle of least privilege is a technique that grants users or systems the minimum level of access or permissions that they need to perform their tasks, and nothing more. By applying the principle of least privilege to a human resources fileshare, the permissions can be restricted to only those who have a legitimate need to access the sensitive data, such as HR staff, managers, or auditors. This can prevent unauthorized users, such as hackers, employees, or contractors, from accessing, copying, modifying, or deleting the data. Therefore, the principle of least privilege can enhance the confidentiality of the data on the fileshare. Integrity, availability, and non-repudiation are other security concepts, but they are not the best reason for permissions on a human resources fileshare to follow the principle of least privilege. Integrity is the security concept that ensures data is accurate and consistent, and protected from unauthorized modification or corruption. Availability is the security concept that ensures data is accessible and usable by authorized users or systems when needed. Non-repudiation is the security concept that ensures the authenticity and accountability of data and actions, and prevents the denial of involvement or responsibility. While these concepts are also important for data security, they are not directly related to the level of access or permissions granted to users or systems.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17, 372-373

139. Security controls in a data center are being reviewed to ensure data is properly protected and that human life considerations are included.

Which of the following best describes how the controls should be set up?

- A. Remote access points should fail closed.
- B. Logging controls should fail open.
- C. Safety controls should fail open.
- D. Logical security controls should fail closed.

Answer: C

Explanation:

Safety controls are security controls that are designed to protect human life and physical assets from harm or damage. Examples of safety controls include fire alarms, sprinklers, emergency exits, backup generators, and surge protectors. Safety controls should fail open, which means that they should remain operational or allow access when a failure or error occurs. Failing open can prevent or minimize the impact of a disaster, such as a fire, flood, earthquake, or power outage, on human life and physical assets. For example, if a fire alarm fails, it should still trigger the sprinklers and unlock the emergency exits, rather than remain silent and locked. Failing open can also ensure that essential services, such as healthcare, transportation, or communication, are available during a crisis. Remote access points, logging controls, and logical security controls are other types of security controls, but they should not fail open in a data center. Remote access points are security controls that allow users or systems to access a network or a system from a remote location, such as a VPN, a web portal, or a wireless access point. Remote access points should fail closed, which means that they should deny access when a failure or error occurs. Failing closed can prevent unauthorized or malicious access to the data center's network or systems, such as by hackers, malware, or rogue devices. Logging controls are security controls that record and monitor the activities and events that occur on a network or a system, such as user actions, system errors, security incidents, or performance metrics. Logging controls should also fail closed, which means that they should stop or suspend the activities or events when a failure or error occurs. Failing closed can prevent data loss, corruption, or tampering, as well as ensure compliance with regulations and standards. Logical security controls are security controls that use software or code to protect data and systems from unauthorized or malicious access, modification, or destruction, such as encryption, authentication, authorization, or firewall. Logical security controls should also fail closed, which means that they should block or restrict access when a failure or error occurs. Failing closed can prevent data breaches, cyberattacks, or logical flaws, as well as ensure confidentiality, integrity, and availability of data and systems.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143, 372-373, 376-377

140. Which of the following is the most common data loss path for an air-gapped network?

- A. Bastion host
- B. Unsecured Bluetooth
- C. Unpatched OS
- D. Removable devices

Answer: D

Explanation:

An air-gapped network is a network that is physically isolated from other networks, such as the internet, to prevent unauthorized access and data leakage. However, an air-gapped network can still be compromised by removable devices, such as USB drives, CDs, DVDs, or external hard drives, that are used to transfer data between the air-gapped network and other networks. Removable devices can carry malware, spyware, or other malicious code that can infect the air-gapped network or exfiltrate data from it. Therefore, removable devices are the most common data loss path for an air-gapped network.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 9: Network Security, page 449 1

141. Which of the following can best protect against an employee inadvertently installing malware on a company system?

- A. Host-based firewall
- B. System isolation
- C. Least privilege
- D. Application allow list

Answer: D

Explanation:

An application allow list is a security technique that specifies which applications are authorized to run on a system and blocks all other applications. An application allow list can best protect against an employee inadvertently installing malware on a company system because it prevents the execution of any unauthorized or malicious software, such as viruses, worms, trojans, ransomware, or spyware. An application allow list can also reduce the attack surface and improve the performance of the system.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 551 1

142. An organization is struggling with scaling issues on its VPN concentrator and internet circuit due to remote work. The organization is looking for a software solution that will allow it to reduce traffic on the VPN and internet circuit, while still providing encrypted tunnel access to the data center and monitoring of remote employee internet traffic.

Which of the following will help achieve these objectives?

- A. Deploying a SASE solution to remote employees
- B. Building a load-balanced VPN solution with redundant internet
- C. Purchasing a low-cost SD-WAN solution for VPN traffic
- D. Using a cloud provider to create additional VPN concentrators

Answer: A

Explanation:

SASE stands for Secure Access Service Edge. It is a cloud-based service that combines network and security functions into a single integrated solution. SASE can help reduce traffic on the VPN and internet circuit by providing secure and optimized access to the data center and cloud applications for remote employees. SASE can also monitor and enforce security policies on the remote employee internet traffic, regardless of their location or device. SASE can offer benefits such as lower costs, improved performance, scalability, and flexibility compared to traditional VPN solutions.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 457-458 1

143. A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS servers, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server.

Which of the following best describes what the security analyst is seeing?

- A. Concurrent session usage
- B. Secure DNS cryptographic downgrade
- C. On-path resource consumption

D. Reflected denial of service

Answer: D

Explanation:

A reflected denial of service (RDoS) attack is a type of DDoS attack that uses spoofed source IP addresses to send requests to a third-party server, which then sends responses to the victim server. The attacker exploits the difference in size between the request and the response, which can amplify the amount of traffic sent to the victim server. The attacker also hides their identity by using the victim's IP address as the source. A RDoS attack can target DNS servers by sending forged DNS queries that generate large DNS responses. This can flood the network interface of the DNS server and prevent it from serving legitimate requests from end users.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 1

144. A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format.

Which of the following should the administrator apply to the site recovery resource group?

- A. RBAC
- B. ACL
- C. SAML
- D. GPO

Answer: A

Explanation:

RBAC stands for Role-Based Access Control, which is a method of restricting access to data and resources based on the roles or responsibilities of users. RBAC simplifies the management of permissions by assigning roles to users and granting access rights to roles, rather than to individual users. RBAC can help enforce the principle of least privilege and reduce the risk of unauthorized access or data leakage. The other options are not as suitable for the scenario as RBAC, as they either do not prevent access based on responsibilities, or do not apply a simplified format.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 133 1

145. One of a company's vendors sent an analyst a security bulletin that recommends a BIOS update. Which of the following vulnerability types is being addressed by the patch?

- A. Virtualization
- B. Firmware
- C. Application
- D. Operating system

Answer: B

Explanation:

Firmware is a type of software that is embedded in hardware devices, such as BIOS, routers, printers, or cameras. Firmware controls the basic functions and operations of the device, and can be updated or patched to fix bugs, improve performance, or enhance security. Firmware vulnerabilities are flaws or weaknesses in the firmware code that can be exploited by attackers to gain unauthorized access, modify settings, or cause damage to the device or the network. A BIOS update is a patch that addresses a firmware vulnerability in the basic input/output system of a computer, which is responsible for booting the

operating system and managing the communication between the hardware and the software. The other options are not types of vulnerabilities, but rather categories of software or technology.

146. A security analyst locates a potentially malicious video file on a server and needs to identify both the creation date and the file's creator.

Which of the following actions would most likely give the security analyst the information required?

- A. Obtain the file's SHA-256 hash.
- B. Use hexdump on the file's contents.
- C. Check endpoint logs.
- D. Query the file's metadata.

Answer: D

Explanation:

Metadata is data that describes other data, such as its format, origin, creation date, author, and other attributes. Video files, like other types of files, can contain metadata that can provide useful information for forensic analysis. For example, metadata can reveal the camera model, location, date and time, and software used to create or edit the video file. To query the file's metadata, a security analyst can use various tools, such as MedialInfo1, ffprobe2, or hexdump3, to extract and display the metadata from the video file. By querying the file's metadata, the security analyst can most likely identify both the creation date and the file's creator, as well as other relevant information. Obtaining the file's SHA-256 hash, checking endpoint logs, or using hexdump on the file's contents are other possible actions, but they are not the most appropriate to answer the question. The file's SHA-256 hash is a cryptographic value that can be used to verify the integrity or uniqueness of the file, but it does not reveal any information about the file's creation date or creator. Checking endpoint logs can provide some clues about the file's origin or activity, but it may not be reliable or accurate, especially if the logs are tampered with or incomplete. Using hexdump on the file's contents can show the raw binary data of the file, but it may not be easy or feasible to interpret the metadata from the hex output, especially if the file is large or encrypted.

Reference: 1: How do I get the meta-data of a video file? 2: How to check if an mp4 file contains malware? 3: [Hexdump - Wikipedia]

147. After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network.

Which of the following is the most appropriate to disable?

- A. Console access
- B. Routing protocols
- C. VLANs
- D. Web-based administration

Answer: D

Explanation:

Web-based administration is a feature that allows users to configure and manage routers through a web browser interface. While this feature can provide convenience and ease of use, it can also pose a security risk, especially if the web interface is exposed to the internet or uses weak authentication or encryption methods. Web-based administration can be exploited by attackers to gain unauthorized access to the router's settings, firmware, or data, or to launch attacks such as cross-site scripting (XSS) or cross-site request forgery (CSRF). Therefore, disabling web-based administration is a good practice to

harden the routers within the corporate network. Console access, routing protocols, and VLANs are other features that can be configured on routers, but they are not the most appropriate to disable for hardening purposes. Console access is a physical connection to the router that requires direct access to the device, which can be secured by locking the router in a cabinet or using a strong password. Routing protocols are essential for routers to exchange routing information and maintain network connectivity, and they can be secured by using authentication or encryption mechanisms. VLANs are logical segments of a network that can enhance network performance and security by isolating traffic and devices, and they can be secured by using VLAN access control lists (VACLs) or private VLANs (PVLANS).

Reference: CCNA SEC: Router Hardening Your Router's Security Stinks: Here's How to Fix It

148. Which of the following should a systems administrator use to ensure an easy deployment of resources within the cloud provider?

- A. Software as a service
- B. Infrastructure as code
- C. Internet of Things
- D. Software-defined networking

Answer: B

Explanation:

Infrastructure as code (IaC) is a method of using code and automation to manage and provision cloud resources, such as servers, networks, storage, and applications. IaC allows for easy deployment, scalability, consistency, and repeatability of cloud environments. IaC is also a key component of DevSecOps, which integrates security into the development and operations processes.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Cloud and Virtualization Concepts, page 294.

149. An enterprise has been experiencing attacks focused on exploiting vulnerabilities in older browser versions with well-known exploits.

Which of the following security solutions should be configured to best provide the ability to monitor and block these known signature-based attacks?

- A. ACL
- B. DLP
- C. IDS
- D. IPS

Answer: D

Explanation:

An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can also perform other functions, such as rate limiting, encryption, or redirection.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

150. During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile.

Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

- A. Federation
- B. Identity proofing
- C. Password complexity
- D. Default password changes
- E. Password manager
- F. Open authentication

Answer: AC

Explanation:

Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them. Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness. Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-313 1

151. An administrator is reviewing a single server's security logs and discovers the following; Which of the following best describes the action captured in this log file?

- A. Brute-force attack
- B. Privilege escalation
- C. Failed password audit
- D. Forgotten password by the user

Answer: A

Explanation:

A brute-force attack is a type of attack that involves systematically trying all possible combinations of passwords or keys until the correct one is found. The log file shows multiple failed login attempts in a short amount of time, which is a characteristic of a brute-force attack. The attacker is trying to guess the password of the Administrator account on the server. The log file also shows the event ID 4625, which indicates a failed logon attempt, and the status code 0xC000006A, which means the user name is correct but the password is wrong. These are indicators of compromise (IoC) that suggest a brute-force attack is taking place.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 and 223 1

152. A security engineer is implementing FDE for all laptops in an organization.

Which of the following are the most important for the engineer to consider as part of the planning process? (Select two).

- A. Key escrow

- B. TPM presence
- C. Digital signatures
- D. Data tokenization
- E. Public key management
- F. Certificate authority linking

Answer: AB

Explanation:

Key escrow is a method of storing encryption keys in a secure location, such as a trusted third party or a hardware security module (HSM). Key escrow is important for FDE because it allows the recovery of encrypted data in case of lost or forgotten passwords, device theft, or hardware failure. Key escrow also enables authorized access to encrypted data for legal or forensic purposes.

TPM presence is a feature of some laptops that have a dedicated chip for storing encryption keys and other security information. TPM presence is important for FDE because it enhances the security and performance of encryption by generating and protecting the keys within the chip, rather than relying on software or external devices. TPM presence also enables features such as secure boot, remote attestation, and device authentication.

153. A hacker gained access to a system via a phishing attempt that was a direct result of a user clicking a suspicious link. The link laterally deployed ransomware, which laid dormant for multiple weeks, across the network.

Which of the following would have mitigated the spread?

- A. IPS
- B. IDS
- C. WAF
- D. UAT

Answer: A

Explanation:

IPS stands for intrusion prevention system, which is a network security device that monitors and blocks malicious traffic in real time. IPS is different from IDS, which only detects and alerts on malicious traffic, but does not block it. IPS would have mitigated the spread of ransomware by preventing the hacker from accessing the system via the phishing link, or by stopping the ransomware from communicating with its command and control server or encrypting the files.

154. A user is attempting to patch a critical system, but the patch fails to transfer.

Which of the following access controls is most likely inhibiting the transfer?

- A. Attribute-based
- B. Time of day
- C. Role-based
- D. Least privilege

Answer: D

Explanation:

The least privilege principle states that users and processes should only have the minimum level of access required to perform their tasks. This helps to prevent unauthorized or unnecessary actions that could compromise security. In this case, the patch transfer might be failing because the user or process

does not have the appropriate permissions to access the critical system or the network resources needed for the transfer. Applying the least privilege principle can help to avoid this issue by granting the user or process the necessary access rights for the patching activity.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 931

155. Which of the following is used to protect a computer from viruses, malware, and Trojans being installed and moving laterally across the network?

- A. IDS
- B. ACL
- C. EDR
- D. NAC

Answer: C

Explanation:

Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints, such as computers, laptops, mobile devices, and servers. EDR can help to detect and prevent malicious software, such as viruses, malware, and Trojans, from infecting the endpoints and spreading across the network. EDR can also provide visibility and response capabilities to contain and remediate threats. EDR is different from IDS, which is a network-based technology that monitors and alerts on network traffic anomalies. EDR is also different from ACL, which is a list of rules that control the access to network resources. EDR is also different from NAC, which is a technology that enforces policies on the network access of devices based on their identity and compliance status.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 2561

156. A systems administrator set up a perimeter firewall but continues to notice suspicious connections between internal endpoints.

Which of the following should be set up in order to mitigate the threat posed by the suspicious activity?

- A. Host-based firewall
- B. Web application firewall
- C. Access control list
- D. Application allow list

Answer: A

Explanation:

A host-based firewall is a software application that runs on an individual endpoint and filters the incoming and outgoing network traffic based on a set of rules. A host-based firewall can help to mitigate the threat posed by suspicious connections between internal endpoints by blocking or allowing the traffic based on the source, destination, port, protocol, or application. A host-based firewall is different from a web application firewall, which is a type of firewall that protects web applications from common web-based attacks, such as SQL injection, cross-site scripting, and session hijacking. A host-based firewall is also different from an access control list, which is a list of rules that control the access to network resources, such as files, folders, printers, or routers. A host-based firewall is also different from an application allow list, which is a list of applications that are authorized to run on an endpoint, preventing unauthorized or malicious applications from executing.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 254

157. A business received a small grant to migrate its infrastructure to an off-premises solution.

Which of the following should be considered first?

- A. Security of cloud providers
- B. Cost of implementation
- C. Ability of engineers
- D. Security of architecture

Answer: D

Explanation:

Security of architecture is the process of designing and implementing a secure infrastructure that meets the business objectives and requirements. Security of architecture should be considered first when migrating to an off-premises solution, such as cloud computing, because it can help to identify and mitigate the potential risks and challenges associated with the migration, such as data security, compliance, availability, scalability, and performance. Security of architecture is different from security of cloud providers, which is the process of evaluating and selecting a trustworthy and reliable cloud service provider that can meet the security and operational needs of the business. Security of architecture is also different from cost of implementation, which is the amount of money required to migrate and maintain the infrastructure in the cloud. Security of architecture is also different from ability of engineers, which is the level of skill and knowledge of the IT staff who are responsible for the migration and management of the cloud infrastructure.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 3491

158. A company is planning a disaster recovery site and needs to ensure that a single natural disaster would not result in the complete loss of regulated backup data.

Which of the following should the company consider?

- A. Geographic dispersion
- B. Platform diversity
- C. Hot site
- D. Load balancing

Answer: A

Explanation:

Geographic dispersion is the practice of having backup data stored in different locations that are far enough apart to minimize the risk of a single natural disaster affecting both sites. This ensures that the company can recover its regulated data in case of a disaster at the primary site. Platform diversity, hot site, and load balancing are not directly related to the protection of backup data from natural disasters.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 449; Disaster Recovery Planning: Geographic Diversity

159. A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours.

Which of the following is most likely occurring?

- A. A worm is propagating across the network.
- B. Data is being exfiltrated.
- C. A logic bomb is deleting data.
- D. Ransomware is encrypting files.

Answer: B

Explanation:

Data exfiltration is a technique that attackers use to steal sensitive data from a target system or network by transmitting it through DNS queries and responses. This method is often used in advanced persistent threat (APT) attacks, in which attackers seek to persistently evade detection in the target environment. A large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours is a strong indicator of data exfiltration. A worm, a logic bomb, and ransomware would not use DNS queries to communicate with their command and control servers or perform their malicious actions.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 487; Introduction to DNS Data Exfiltration; Identifying a DNS Exfiltration Attack That Wasn't Real — This Time

160. An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards.

Which of the following types of attacks does this describe?

- A. Vishing
- B. Smishing
- C. Pretexting
- D. Phishing

Answer: B

Explanation:

Smishing is a type of phishing attack that uses text messages or common messaging apps to trick victims into clicking on malicious links or providing personal information. The scenario in the question describes a smishing attack that uses pretexting, which is a form of social engineering that involves impersonating someone else to gain trust or access. The unknown number claims to be the company's CEO and asks the employee to purchase gift cards, which is a common scam tactic. Vishing is a similar type of attack that uses phone calls or voicemails, while phishing is a broader term that covers any email-based attack.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 771; Smishing vs. Phishing: Understanding the Differences2

161. Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

- A. A full inventory of all hardware and software
- B. Documentation of system classifications
- C. A list of system owners and their departments
- D. Third-party risk assessment documentation

Answer: A

Explanation:

A full inventory of all hardware and software is essential for measuring the overall risk to an organization when a new vulnerability is disclosed, because it allows the security analyst to identify which systems are affected by the vulnerability and prioritize the remediation efforts. Without a full inventory, the security analyst may miss some vulnerable systems or waste time and resources on irrelevant ones.

Documentation of system classifications, a list of system owners and their departments, and third-party

risk assessment documentation are all useful for risk management, but they are not sufficient to measure the impact of a new vulnerability.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; Risk Assessment and Analysis Methods: Qualitative and Quantitative3

162. A systems administrator is changing the password policy within an enterprise environment and wants this update implemented on all systems as quickly as possible.

Which of the following operating system security measures will the administrator most likely use?

- A. Deploying PowerShell scripts
- B. Pushing GPO update
- C. Enabling PAP
- D. Updating EDR profiles

Answer: B

Explanation:

A group policy object (GPO) is a mechanism for applying configuration settings to computers and users in an Active Directory domain. By pushing a GPO update, the systems administrator can quickly and uniformly enforce the new password policy across all systems in the domain. Deploying PowerShell scripts, enabling PAP, and updating EDR profiles are not the most efficient or effective ways to change the password policy within an enterprise environment.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 115; Password Policy - Windows Security

163. A company is planning to set up a SIEM system and assign an analyst to review the logs on a weekly basis Which of the following types of controls is the company setting up?

- A. Corrective
- B. Preventive
- C. Detective
- D. Deterrent

Answer: C

Explanation:

A detective control is a type of security control that monitors and analyzes events to detect and report on potential or actual security incidents. A SIEM system is an example of a detective control, as it collects, correlates, and analyzes security data from various sources and generates alerts for security teams. Corrective, preventive, and deterrent controls are different types of security controls that aim to restore, protect, or discourage security breaches, respectively.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 33; What is Security Information and Event Management (SIEM)?

164. Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule.

Which of the following but describes this form of security control?

- A. Physical
- B. Managerial
- C. Technical

D. Operational

Answer: A

Explanation:

A physical security control is a device or mechanism that prevents unauthorized access to a physical location or asset. An access control vestibule, also known as a mantrap, is a physical security control that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens. This prevents unauthorized individuals from following authorized individuals into the facility, a practice known as piggybacking or tailgating. A photo ID check is another form of physical security control that verifies the identity of visitors. Managerial, technical, and operational security controls are not directly related to physical access, but rather to policies, procedures, systems, and processes that support security objectives.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 341; Mantrap (access control) - Wikipedia2

165. A company must ensure sensitive data at rest is rendered unreadable.

Which of the following will the company most likely use?

- A. Hashing
- B. Tokenization
- C. Encryption
- D. Segmentation

Answer: C

Explanation:

Encryption is a method of transforming data in a way that makes it unreadable without a secret key necessary to decrypt the data back into plaintext. Encryption is one of the most common and effective ways to protect data at rest, as it prevents unauthorized access, modification, or theft of the data.

Encryption can be applied to different types of data at rest, such as block storage, object storage, databases, archives, and so on. Hashing, tokenization, and segmentation are not methods of rendering data at rest unreadable, but rather of protecting data in other ways. Hashing is a one-way function that generates a fixed-length output, called a hash or digest, from an input, such that the input cannot be recovered from the output. Hashing is used to verify the integrity and authenticity of data, but not to encrypt it. Tokenization is a process that replaces sensitive data with non-sensitive substitutes, called tokens, that have no meaning or value on their own. Tokenization is used to reduce the exposure and compliance scope of sensitive data, but not to encrypt it. Segmentation is a technique that divides a network or a system into smaller, isolated units, called segments, that have different levels of access and security. Segmentation is used to limit the attack surface and contain the impact of a breach, but not to encrypt data at rest.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, pages 77-781; Protecting data at rest - Security Pillar3

166. Which of the following describes the maximum allowance of accepted risk?

- A. Risk indicator
- B. Risk level
- C. Risk score
- D. Risk threshold

Answer: D

Explanation:

Risk threshold is the maximum amount of risk that an organization is willing to accept for a given activity or decision. It is also known as risk appetite or risk tolerance. Risk threshold helps an organization to prioritize and allocate resources for risk management. Risk indicator, risk level, and risk score are different ways of measuring or expressing the likelihood and impact of a risk, but they do not describe the maximum allowance of accepted risk.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 34; Accepting Risk: Definition, How It Works, and Alternatives

167. Which of the following incident response activities ensures evidence is properly handled?

- A. E-discovery
- B. Chain of custody
- C. Legal hold
- D. Preservation

Answer: B

Explanation:

Chain of custody is the process of documenting and preserving the integrity of evidence collected during an incident response. It involves recording the details of each person who handled the evidence, the time and date of each transfer, and the location where the evidence was stored. Chain of custody ensures that the evidence is admissible in legal proceedings and can be traced back to its source. E-discovery, legal hold, and preservation are related concepts, but they do not ensure evidence is properly handled.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 487; NIST SP 800-61: 3.2. Evidence Gathering and Handling

168. Which of the following risk management strategies should an enterprise adopt first if a legacy application is critical to business operations and there are preventative controls that are not yet implemented?

- A. Mitigate
- B. Accept
- C. Transfer
- D. Avoid

Answer: A

Explanation:

Mitigate is the risk management strategy that involves reducing the likelihood or impact of a risk. If a legacy application is critical to business operations and there are preventative controls that are not yet implemented, the enterprise should adopt the mitigate strategy first to address the existing vulnerabilities and gaps in the application. This could involve applying patches, updates, or configuration changes to the application, or adding additional layers of security controls around the application. Accept, transfer, and avoid are other risk management strategies, but they are not the best options for this scenario. Accept means acknowledging the risk and accepting the consequences without taking any action. Transfer means shifting the risk to a third party, such as an insurance company or a vendor. Avoid means eliminating the risk by removing the source or changing the process. These strategies may not be

feasible or desirable for a legacy application that is critical to business operations and has no preventative controls in place.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; A Risk-Based Framework for Legacy System Migration and Deprecation²

169. Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

- A. Red
- B. Blue
- C. Purple
- D. Yellow

Answer: C

Explanation:

Purple is the team that combines both offensive and defensive testing techniques to protect an organization's critical systems. Purple is not a separate team, but rather a collaboration between the red team and the blue team. The red team is the offensive team that simulates attacks and exploits vulnerabilities in the organization's systems. The blue team is the defensive team that monitors and protects the organization's systems from real and simulated threats. The purple team exists to ensure and maximize the effectiveness of the red and blue teams by integrating the defensive tactics and controls from the blue team with the threats and vulnerabilities found by the red team into a single narrative that improves the overall security posture of the organization. Red, blue, and yellow are other types of teams involved in security testing, but they do not combine both offensive and defensive techniques. The yellow team is the team that builds software solutions, scripts, and other programs that the blue team uses in the security testing.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1331; Penetration Testing: Understanding Red, Blue, & Purple Teams³

170. A company is working with a vendor to perform a penetration test Which of the following includes an estimate about the number of hours required to complete the engagement?

- A. SOW
- B. BPA
- C. SLA
- D. NDA

Answer: A

Explanation:

A statement of work (SOW) is a document that defines the scope, objectives, deliverables, timeline, and costs of a project or service. It typically includes an estimate of the number of hours required to complete the engagement, as well as the roles and responsibilities of the parties involved. A SOW is often used for penetration testing projects to ensure that both the client and the vendor have a clear and mutual understanding of what is expected and how the work will be performed. A business partnership agreement (BPA), a service level agreement (SLA), and a non-disclosure agreement (NDA) are different types of contracts that may be related to a penetration testing project, but they do not include an estimate of the number of hours required to complete the engagement.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 492; What to Look For in a Penetration Testing Statement of Work?

171. The local administrator account for a company's VPN appliance was unexpectedly used to log in to the remote management interface.

Which of the following would have most likely prevented this from happening'?

- A. Using least privilege
- B. Changing the default password
- C. Assigning individual user IDs
- D. Reviewing logs more frequently

Answer: B

Explanation:

Changing the default password for the local administrator account on a VPN appliance is a basic security measure that would have most likely prevented the unexpected login to the remote management interface. Default passwords are often easy to guess or publicly available, and attackers can use them to gain unauthorized access to devices and systems. Changing the default password to a strong and unique one reduces the risk of brute-force attacks and credential theft. Using least privilege, assigning individual user IDs, and reviewing logs more frequently are also good security practices, but they are not as effective as changing the default password in preventing the unexpected login.

Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 116; Local Admin Accounts - Security Risks and Best Practices (Part 1)

172. Which of the following would be most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk?

- A. ARO
- B. RTO
- C. RPO
- D. ALE
- E. SLE

Answer: D

Explanation:

The Annual Loss Expectancy (ALE) is most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk. ALE is calculated by multiplying the Single Loss Expectancy (SLE) by the Annualized Rate of Occurrence (ARO), which provides an estimate of the annual expected loss due to a specific risk, making it valuable for long-term financial planning and risk management decisions.

Reference: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

173. A security analyst is investigating an application server and discovers that software on the server is behaving abnormally. The software normally runs batch jobs locally and does not generate traffic, but the process is now generating outbound traffic over random high ports.

Which of the following vulnerabilities has likely been exploited in this software?

- A. Memory injection
- B. Race condition

- C. Side loading
- D. SQL injection

Answer: A

Explanation:

Memory injection vulnerabilities allow unauthorized code or commands to be executed within a software program, leading to abnormal behavior such as generating outbound traffic over random high ports. This issue often arises from software not properly validating or encoding input, which can be exploited by attackers to inject malicious code.

Reference: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

174. A company wants to verify that the software the company is deploying came from the vendor the company purchased the software from.

Which of the following is the best way for the company to confirm this information?

- A. Validate the code signature.
- B. Execute the code in a sandbox.
- C. Search the executable for ASCII strings.
- D. Generate a hash of the files.

Answer: A

Explanation:

Validating the code signature is the best way to verify software authenticity, as it ensures that the software has not been tampered with and that it comes from a verified source. Code signatures are digital signatures applied by the software vendor, and validating them confirms the software's integrity and origin.

Reference: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

175. In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password.

Which of the following best describes this technique?

- A. Key stretching
- B. Tokenization
- C. Data masking
- D. Salting

Answer: D

Explanation:

Adding a random string of characters, known as a "salt," to a password before hashing it is known as salting. This technique strengthens passwords by ensuring that even if two users have the same password, their hashes will be different due to the unique salt, making it much harder for attackers to crack passwords using precomputed tables.

Reference: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

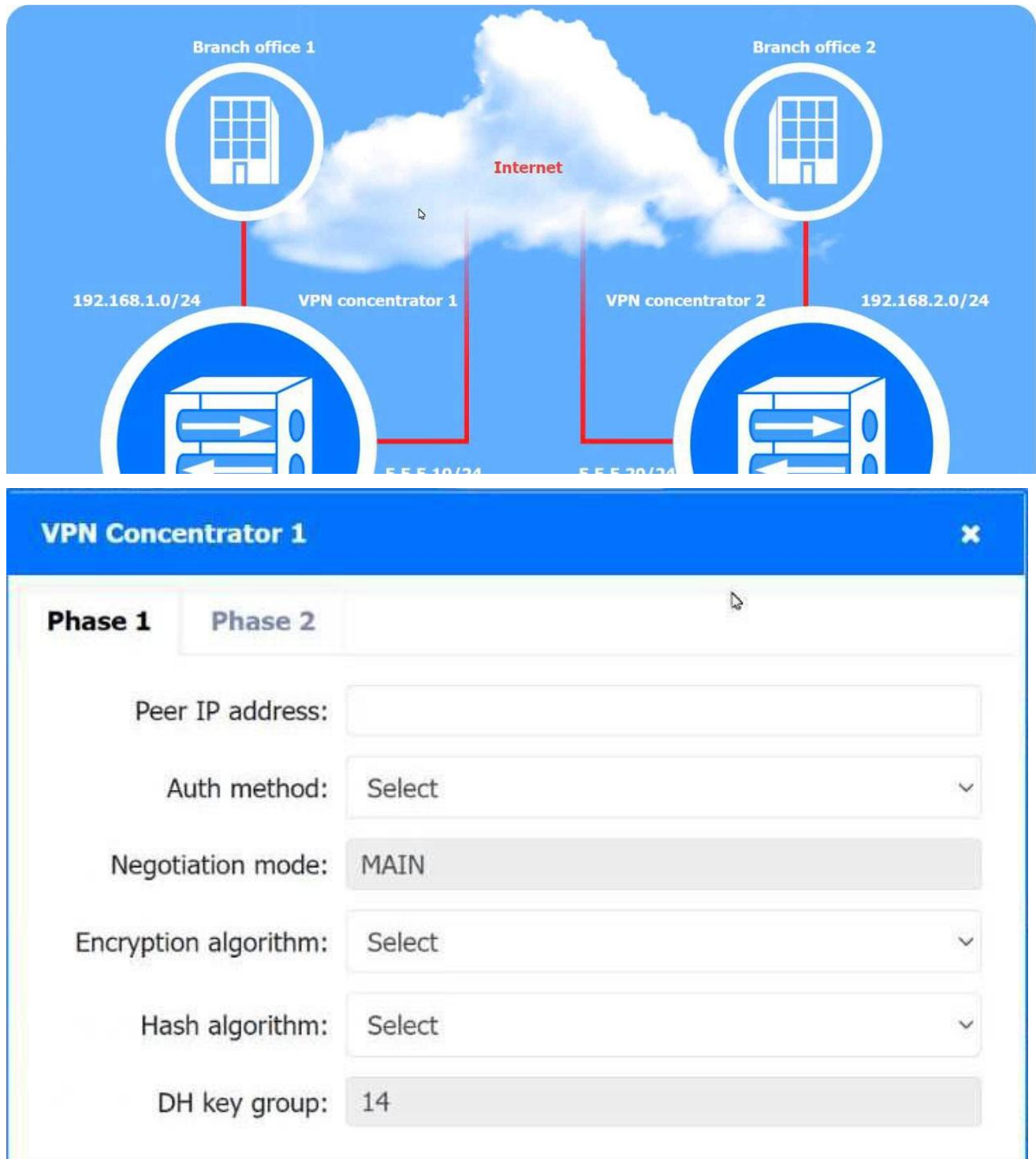
176. SIMULATION

A systems administrator is configuring a site-to-site VPN between two branch offices. Some of the settings have already been configured correctly.

The systems administrator has been provided the following requirements as part of completing the

configuration:

- Most secure algorithms should be selected
- All traffic should be encrypted over the VPN
- A secret password will be used to authenticate the two VPN concentrators



VPN Concentrator 1 ✕

Phase 1 **Phase 2**

Mode: Tunnel

Protocol: ESP

Encryption algorithm: AES256

Hash algorithm: SHA256

Local network/mask: 192.168.1.0/24

Remote network/mask: 192.168.2.0/24

Reset to Default

Save

Close

VPN Concentrator 2 ✕

Phase 1 **Phase 2**

Peer IP address: 5.5.5.10

Auth method: PSK

Negotiation mode: MAIN

Encryption algorithm: AES256

Hash algorithm: SHA256

DH key group: 14

Reset to Default

Save

Close

VPN Concentrator 2

Phase 1 **Phase 2**

Mode: Tunnel

Protocol: ESP

Encryption algorithm: AES256

Hash algorithm: SHA256

Local network/mask: 192.168.2.0/24

Remote network/mask: 192.168.1.0/24

Reset to Default Save Close

Answer:

To configure the site-to-site VPN between the two branch offices according to the provided requirements, here are the detailed steps and settings that need to be applied to the VPN concentrators:

Requirements:

Most secure algorithms should be selected.

All traffic should be encrypted over the VPN.

A secret password will be used to authenticate the two VPN concentrators.

VPN Concentrator 1 Configuration:

Phase 1:

Peer IP address: 5.5.5.10 (The IP address of VPN Concentrator 2)

Auth method: PSK (Pre-Shared Key)

Negotiation mode: MAIN

Encryption algorithm: AES256

Hash algorithm: SHA256

DH key group: 14

Phase 2:

Mode: Tunnel

Protocol: ESP (Encapsulating Security Payload)

Encryption algorithm: AES256

Hash algorithm: SHA256

Local network/mask: 192.168.1.0/24

Remote network/mask: 192.168.2.0/24

VPN Concentrator 2 Configuration:

Phase 1:

Peer IP address: 5.5.5.5 (The IP address of VPN Concentrator 1)

Auth method: PSK (Pre-Shared Key)

Negotiation mode: MAIN

Encryption algorithm: AES256

Hash algorithm: SHA256

DH key group: 14

Phase 2:

Mode: Tunnel

Protocol: ESP (Encapsulating Security Payload)

Encryption algorithm: AES256

Hash algorithm: SHA256

Local network/mask: 192.168.2.0/24

Remote network/mask: 192.168.1.0/24

Summary:

Peer IP Address: Set to the IP address of the remote VPN concentrator.

Auth Method: PSK for using a pre-shared key.

Negotiation Mode: MAIN for the initial setup.

Encryption Algorithm: AES256, which is a strong and secure algorithm.

Hash Algorithm: SHA256, which provides strong hashing.

DH Key Group: 14 for strong Diffie-Hellman key exchange.

Phase 2 Protocol: ESP for encryption and integrity.

Local and Remote Networks: Properly configure the local and remote network addresses to match each branch office subnet.

By configuring these settings on both VPN concentrators, the site-to-site VPN will meet the requirements for strong security algorithms, encryption of all traffic, and authentication using a pre-shared key.

177. Which of the following security concepts is accomplished with the installation of a RADIUS server?

- A. CIA
- B. AAA
- C. ACL
- D. PEM

Answer: B

Explanation:

The installation of a RADIUS server (Remote Authentication Dial-In User Service) is primarily associated with the security concept of AAA, which stands for Authentication, Authorization, and Accounting. RADIUS servers are used to manage user credentials and permissions centrally, ensuring that only authenticated and authorized users can access network resources, and tracking user activity for accounting purposes.

Authentication: Verifies the identity of a user or device. When a user tries to access a network, the RADIUS server checks their credentials (username and password) against a database.

Authorization: Determines what an authenticated user is allowed to do. After authentication, the RADIUS server grants permissions based on predefined policies.

Accounting: Tracks the consumption of network resources by users. This involves logging session details such as the duration of connections and the amount of data transferred.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.6 - Implement and maintain identity and access management.

178. A software developer released a new application and is distributing application files via the developer's website.

Which of the following should the developer post on the website to allow users to verify the integrity of the downloaded files?

- A. Hashes
- B. Certificates
- C. Algorithms
- D. Salting

Answer: A

Explanation:

To verify the integrity of downloaded files, a software developer should post hashes on the website. A hash is a fixed-length string or number generated from input data, such as a file. When users download the application files, they can generate their own hash from the downloaded files and compare it with the hash provided by the developer. If the hashes match, it confirms that the files have not been altered or corrupted during the download process.

Hashes: Ensure data integrity by allowing users to verify that the downloaded files are identical to the original ones. Common hashing algorithms include MD5, SHA-1, and SHA-256.

Certificates and Algorithms: Are more related to ensuring authenticity and securing communications rather than verifying file integrity.

Salting: Is a technique used in hashing passwords to add an additional layer of security, not for verifying file integrity.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2 - Summarize fundamental security concepts (Hashing).

179. A company tested and validated the effectiveness of network security appliances within the corporate network. The IDS detected a high rate of SQL injection attacks against the company's servers, and the company's perimeter firewall is at capacity.

Which of the following would be the best action to maintain security and reduce the traffic to the perimeter firewall?

- A. Set the appliance to IPS mode and place it in front of the company firewall.
- B. Convert the firewall to a WAF and use IPSec tunnels to increase throughput.
- C. Set the firewall to fail open if it is overloaded with traffic and send alerts to the SIEM.
- D. Configure the firewall to perform deep packet inspection and monitor TLS traffic.

Answer: A

Explanation:

Given the scenario where an Intrusion Detection System (IDS) has detected a high rate of SQL injection attacks and the perimeter firewall is at capacity, the best action would be to set the appliance to Intrusion Prevention System (IPS) mode and place it in front of the company firewall.

This approach has several benefits:

Intrusion Prevention System (IPS): Unlike IDS, which only detects and alerts on malicious activity, IPS can actively block and prevent those activities. Placing an IPS in front of the firewall means it can filter out malicious traffic before it reaches the firewall, reducing the load on the firewall and enhancing overall security.

Reducing Traffic Load: By blocking SQL injection attacks and other malicious traffic before it reaches the firewall, the IPS helps maintain the firewall's performance and prevents it from becoming a bottleneck.

Enhanced Security: The IPS provides an additional layer of defense, identifying and mitigating threats in real-time.

Option B (Convert the firewall to a WAF and use IPSec tunnels) would not address the primary issue of reducing traffic to the firewall effectively. Option C (Set the firewall to fail open) would compromise security. Option D (Deep packet inspection) could be resource-intensive and might not alleviate the firewall capacity issue effectively.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5 - Mitigation techniques used to secure the enterprise.

180. A systems administrator is working on a defense-in-depth strategy and needs to restrict activity from employees after hours.

Which of the following should the systems administrator implement?

- A. Role-based restrictions
- B. Attribute-based restrictions
- C. Mandatory restrictions
- D. Time-of-day restrictions

Answer: D

Explanation:

To restrict activity from employees after hours, the systems administrator should implement time-of-day restrictions. This method allows access to network resources to be limited to specific times, ensuring that employees can only access systems during approved working hours. This is an effective part of a defense-in-depth strategy to mitigate risks associated with unauthorized access during off-hours, which could be a time when security monitoring might be less stringent.

Time-of-day restrictions: These control access based on the time of day, preventing users from logging in or accessing certain systems outside of designated hours.

Role-based restrictions: Control access based on a user's role within the organization.

Attribute-based restrictions: Use various attributes (such as location, department, or project) to determine access rights.

Mandatory restrictions: Typically refer to non-discretionary access controls, such as those based on government or organizational policy.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.6 - Implement and maintain identity and access management (Access controls: Time-of-day restrictions).

181. An organization maintains intellectual property that it wants to protect.

Which of the following concepts would be most beneficial to add to the company's security awareness training program?

- A. Insider threat detection
- B. Simulated threats

- C. Phishing awareness
- D. Business continuity planning

Answer: A

Explanation:

For an organization that wants to protect its intellectual property, adding insider threat detection to the security awareness training program would be most beneficial. Insider threats can be particularly dangerous because they come from trusted individuals within the organization who have legitimate access to sensitive information.

Insider threat detection: Focuses on identifying and mitigating threats from within the organization, including employees, contractors, or business partners who might misuse their access.

Simulated threats: Often used for testing security measures and training, but not specifically focused on protecting intellectual property.

Phishing awareness: Important for overall security but more focused on preventing external attacks rather than internal threats.

Business continuity planning: Ensures the organization can continue operations during and after a disruption but does not directly address protecting intellectual property from insider threats.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.6 - Implement security awareness practices (Insider threat detection).

182. Which of the following risks can be mitigated by HTTP headers?

- A. SQLi
- B. XSS
- C. DoS
- D. SSL

Answer: B

Explanation:

HTTP headers can be used to mitigate risks associated with Cross-Site Scripting (XSS). Security-related HTTP headers such as Content Security Policy (CSP) and X-XSS-Protection can be configured to prevent the execution of malicious scripts in the context of a web page.

XSS (Cross-Site Scripting): A vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. HTTP headers like CSP help prevent XSS attacks by specifying which dynamic resources are allowed to load.

SQLi (SQL Injection): Typically mitigated by using parameterized queries and input validation, not HTTP headers.

DoS (Denial of Service): Mitigated by network and application-level defenses rather than HTTP headers.

SSL (Secure Sockets Layer): Refers to securing communications and is not directly mitigated by HTTP headers; rather, it's implemented using SSL/TLS protocols.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 3.3 - Protect data (HTTP headers for securing web applications).

183. Which of the following describes the category of data that is most impacted when it is lost?

- A. Confidential
- B. Public
- C. Private

D. Critical

Answer: D

Explanation:

The category of data that is most impacted when it is lost is "Critical." Critical data is essential to the organization's operations and often includes sensitive information such as financial records, proprietary business information, and vital operational data. The loss of critical data can severely disrupt business operations and have significant financial, legal, and reputational consequences.

Confidential: Refers to data that must be protected from unauthorized access to maintain privacy and security.

Public: Refers to data that is intended for public disclosure and whose loss does not have severe consequences.

Private: Typically refers to personal data that needs to be protected to ensure privacy.

Critical: Refers to data that is essential for the operation and survival of the organization, and its loss can have devastating impacts.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.2 - Risk management (Critical data identification and impact analysis).

184. After performing an assessment, an analyst wants to provide a risk rating for the findings.

Which of the following concepts should most likely be considered when calculating the ratings?

- A. Owners and thresholds
- B. Impact and likelihood
- C. Appetite and tolerance
- D. Probability and exposure factor

Answer: B

Explanation:

When calculating risk ratings, the concepts of impact and likelihood are most likely to be considered.

Risk assessment typically involves evaluating the potential impact of a threat (how severe the consequences would be if the threat materialized) and the likelihood of the threat occurring (how probable it is that the threat will occur).

Impact: Measures the severity of the consequences if a particular threat exploits a vulnerability. It considers factors such as financial loss, reputational damage, and operational disruption.

Likelihood: Measures the probability of a threat exploiting a vulnerability. This can be based on historical data, current threat landscape, and expert judgment.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.2 - Risk management process (Risk assessment: impact and likelihood).

185. Which of the following should a systems administrator set up to increase the resilience of an application by splitting the traffic between two identical sites?

- A. Load balancing
- B. Geographic disruption
- C. Failover
- D. Parallel processing

Answer: A

Explanation:

To increase the resilience of an application by splitting the traffic between two identical sites, a systems administrator should set up load balancing. Load balancing distributes network or application traffic across multiple servers or sites, ensuring no single server becomes overwhelmed and enhancing the availability and reliability of applications.

Load balancing: Distributes traffic across multiple servers to ensure high availability and reliability. It helps in managing the load efficiently and can prevent server overloads.

Geographic disruption: Not a standard term related to resilience. This might imply the use of geographically distributed sites but isn't the precise solution described.

Failover: Refers to switching to a standby server or system when the primary one fails. It doesn't inherently split traffic but rather takes over when a failure occurs.

Parallel processing: Refers to the simultaneous processing of tasks, not specifically related to load balancing web traffic.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.4 - Security operations
(Enhancing security capabilities: load balancing).

186. An organization would like to calculate the time needed to resolve a hardware issue with a server. Which of the following risk management processes describes this example?

- A. Recovery point objective
- B. Mean time between failures
- C. Recovery time objective
- D. Mean time to repair

Answer: D

Explanation:

Mean time to repair (MTTR) describes the time needed to resolve a hardware issue with a server. MTTR is a key metric in risk management and maintenance that measures the average time required to repair a failed component or system and restore it to operational status.

Recovery point objective (RPO): Defines the maximum acceptable amount of data loss measured in time. It is the point in time to which data must be restored after a disaster.

Mean time between failures (MTBF): Measures the average time between failures of a system or component, indicating reliability.

Recovery time objective (RTO): Defines the maximum acceptable length of time to restore a system after a disaster or disruption.

Mean time to repair (MTTR): Measures the average time required to repair a failed component or system.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.2 - Risk management process (MTTR).

187. Which of the following is most likely to be deployed to obtain and analyze attacker activity and techniques?

- A. Firewall
- B. IDS
- C. Honeypot
- D. Layer 3 switch

Answer: C

Explanation:

A honeypot is most likely to be deployed to obtain and analyze attacker activity and techniques. A honeypot is a decoy system set up to attract attackers, providing an opportunity to study their methods and behaviors in a controlled environment without risking actual systems.

Honeypot: A decoy system designed to lure attackers, allowing administrators to observe and analyze attack patterns and techniques.

Firewall: Primarily used to block unauthorized access to networks, not for observing attacker behavior.

IDS (Intrusion Detection System): Detects and alerts on malicious activity but does not specifically engage attackers to observe their behavior.

Layer 3 switch: Used for routing traffic within networks, not for analyzing attacker techniques.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 2.4 - Indicators of malicious activity (Honeypots).

188. Which of the following would most likely mitigate the impact of an extended power outage on a company's environment?

- A. Hot site
- B. UPS
- C. Snapshots
- D. SOAR

Answer: B

Explanation:

A UPS (Uninterruptible Power Supply) would most likely mitigate the impact of an extended power outage on a company's environment. A UPS provides backup power and ensures that systems continue to run during short-term power outages, giving enough time to perform an orderly shutdown or switch to a longer-term power solution like a generator.

Hot site: A fully operational offsite data center that can be used if the primary site becomes unavailable. It's more suitable for disaster recovery rather than mitigating short-term power outages.

UPS: Provides immediate backup power, protecting against data loss and hardware damage during power interruptions.

Snapshots: Used for data backup and recovery, not for power outage mitigation.

SOAR (Security Orchestration, Automation, and Response): A platform for automating security operations, not related to power outage mitigation.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 3.4 - Importance of resilience and recovery in security architecture (Power: Generators, UPS).

189. A security analyst is investigating an alert that was produced by endpoint protection software. The analyst determines this event was a false positive triggered by an employee who attempted to download a file.

Which of the following is the most likely reason the download was blocked?

- A. A misconfiguration in the endpoint protection software
- B. A zero-day vulnerability in the file
- C. A supply chain attack on the endpoint protection vendor
- D. Incorrect file permissions

Answer: A

Explanation:

The most likely reason the download was blocked, resulting in a false positive, is a misconfiguration in the endpoint protection software. False positives occur when legitimate actions are incorrectly identified as threats due to incorrect settings or overly aggressive rules in the security software.

Misconfiguration in the endpoint protection software: Common cause of false positives, where legitimate activities are flagged incorrectly due to improper settings.

Zero-day vulnerability: Refers to previously unknown vulnerabilities, which are less likely to be associated with a false positive.

Supply chain attack: Involves compromising the software supply chain, which is a broader and more severe issue than a simple download being blocked.

Incorrect file permissions: Would prevent access to files but not typically cause an alert in endpoint protection software.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.3 - Explain various activities associated with vulnerability management (False positives).

190. An organization is required to maintain financial data records for three years and customer data for five years.

Which of the following data management policies should the organization implement?

- A. Retention
- B. Destruction
- C. Inventory
- D. Certification

Answer: A

Explanation:

The organization should implement a retention policy to ensure that financial data records are kept for three years and customer data for five years. A retention policy specifies how long different types of data should be maintained and when they should be deleted.

Retention: Ensures that data is kept for a specific period to comply with legal, regulatory, or business requirements.

Destruction: Involves securely deleting data that is no longer needed, which is part of the retention lifecycle but not the primary focus here.

Inventory: Involves keeping track of data assets, not specifically about how long to retain data.

Certification: Ensures that processes and systems meet certain standards, not directly related to data retention periods.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.2 - Risk management process (Data retention).

191. department is not using the company VPN when accessing various company-related services and systems.

Which of the following scenarios describes this activity?

- A. Espionage
- B. Data exfiltration
- C. Nation-state attack
- D. Shadow IT

Answer: D

Explanation:

The activity described, where a department is not using the company VPN when accessing various company-related services and systems, is an example of Shadow IT. Shadow IT refers to the use of IT systems, devices, software, applications, and services without explicit IT department approval.

Espionage: Involves spying to gather confidential information, not simply bypassing the VPN.

Data exfiltration: Refers to unauthorized transfer of data, which might involve not using a VPN but is more specific to the act of transferring data out of the organization.

Nation-state attack: Involves attacks sponsored by nation-states, which is not indicated in the scenario.

Shadow IT: Use of unauthorized systems and services, which aligns with bypassing the company VPN.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 2.1 - Compare and contrast common threat actors and motivations (Shadow IT).

192. Which of the following is classified as high availability in a cloud environment?

- A. Access broker
- B. Cloud HSM
- C. WAF
- D. Load balancer

Answer: D

Explanation:

In a cloud environment, high availability is typically ensured through the use of a load balancer. A load balancer distributes network or application traffic across multiple servers, ensuring that no single server becomes overwhelmed and that services remain available even if one or more servers fail. This setup enhances the reliability and availability of applications.

Load balancer: Ensures high availability by distributing traffic across multiple servers or instances, preventing overload and ensuring continuous availability.

Access broker: Typically refers to a service that facilitates secure access to resources, not directly related to high availability.

Cloud HSM (Hardware Security Module): Provides secure key management in the cloud but does not specifically ensure high availability.

WAF (Web Application Firewall): Protects web applications by filtering and monitoring HTTP traffic but is not primarily focused on ensuring high availability.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.4 - Security operations (Load balancing for high availability).

193. Which of the following is the best way to secure an on-site data center against intrusion from an insider?

- A. Bollards
- B. Access badge
- C. Motion sensor
- D. Video surveillance

Answer: B

Explanation:

To secure an on-site data center against intrusion from an insider, the best measure is to use an access

badge system. Access badges control who can enter restricted areas by verifying their identity and permissions, thereby preventing unauthorized access from insiders.

Access badge: Provides controlled and monitored access to restricted areas, ensuring that only authorized personnel can enter.

Bollards: Provide physical barriers to prevent vehicle access but do not prevent unauthorized personnel entry.

Motion sensor: Detects movement but does not control or restrict access.

Video surveillance: Monitors and records activity but does not physically prevent intrusion.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2 - Summarize fundamental security concepts (Physical security controls).

194. An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions to use a new account.

Which of the following would most likely prevent this activity in the future?

- A. Standardizing security incident reporting
- B. Executing regular phishing campaigns
- C. Implementing insider threat detection measures
- D. Updating processes for sending wire transfers

Answer: D

Explanation:

To prevent an accounting clerk from sending money to an attacker's bank account due to fraudulent instructions, the most effective measure would be updating the processes for sending wire transfers. This can include implementing verification steps, such as requiring multiple approvals for changes in payment instructions and directly confirming new account details with trusted sources.

Updating processes for sending wire transfers: Involves adding verification and approval steps to prevent fraudulent transfers.

Standardizing security incident reporting: Important for handling incidents but not specifically focused on preventing fraudulent wire transfers.

Executing regular phishing campaigns: Helps raise awareness but may not directly address the process vulnerability.

Implementing insider threat detection measures: Useful for detecting malicious activities but does not directly prevent fraudulent transfer instructions.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.6 - Implement security awareness practices (Updating processes).

195. The CIRT is reviewing an incident that involved a human resources recruiter exfiltration sensitive company data. The CIRT found that the recruiter was able to use HTTP over port 53 to upload documents to a web server.

Which of the following security infrastructure devices could have identified and blocked this activity?

- A. WAF utilizing SSL decryption
- B. NGFW utilizing application inspection
- C. UTM utilizing a threat feed
- D. SD-WAN utilizing IPSec

Answer: B

Explanation:

An NGFW (Next-Generation Firewall) utilizing application inspection could have identified and blocked the unusual use of HTTP over port 53. Application inspection allows NGFWs to analyze traffic at the application layer, identifying and blocking suspicious or non-standard protocol usage, such as HTTP traffic on DNS port 53.

NGFW utilizing application inspection: Inspects traffic at the application layer and can block non-standard protocol usage, such as HTTP over port 53.

WAF utilizing SSL decryption: Focuses on protecting web applications and decrypting SSL traffic but may not detect the use of HTTP over port 53.

UTM utilizing a threat feed: Provides comprehensive security but may not focus specifically on application layer inspection.

SD-WAN utilizing IPSec: Enhances secure WAN connections but is not primarily designed to inspect and block specific application traffic.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.5 - Modify enterprise capabilities to enhance security (Next-generation firewall).

196. Which of the following most impacts an administrator's ability to address CVEs discovered on a server?

- A. Rescanning requirements
- B. Patch availability
- C. Organizational impact
- D. Risk tolerance

Answer: B

Explanation:

Patch availability most impacts an administrator's ability to address Common Vulnerabilities and Exposures (CVEs) discovered on a server. If a patch is not available for a discovered vulnerability, the administrator cannot remediate the issue directly through patching, which leaves the system exposed until a patch is released.

Patch availability: Directly determines whether a discovered vulnerability can be fixed promptly. Without available patches, administrators must look for other mitigation strategies.

Rescanning requirements: Important for verifying the effectiveness of patches but secondary to the availability of the patches themselves.

Organizational impact: Considers the potential consequences of vulnerabilities but does not directly impact the ability to apply patches.

Risk tolerance: Influences how the organization prioritizes addressing vulnerabilities but does not affect the actual availability of patches.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 2.3 - Explain various types of vulnerabilities (Patch management).

197. After conducting a vulnerability scan, a systems administrator notices that one of the identified vulnerabilities is not present on the systems that were scanned.

Which of the following describes this example?

- A. False positive
- B. False negative

- C. True positive
- C. True negative

Answer: A

Explanation:

A false positive occurs when a vulnerability scan identifies a vulnerability that is not actually present on the systems that were scanned. This means that the scan has incorrectly flagged a system as vulnerable.

False positive: Incorrectly identifies a vulnerability that does not exist on the scanned systems.

False negative: Fails to identify an existing vulnerability on the system.

True positive: Correctly identifies an existing vulnerability.

True negative: Correctly identifies that there is no vulnerability.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.3 - Explain various activities associated with vulnerability management (False positives and false negatives).

198. Which of the following best describes configuring devices to log to an off-site location for possible future reference?

- A. Log aggregation
- B. DLP
- C. Archiving
- D. SCAP

Answer: A

Explanation:

Configuring devices to log to an off-site location for possible future reference is best described as log aggregation. Log aggregation involves collecting logs from multiple sources and storing them in a centralized location, often off-site, to ensure they are preserved and can be analyzed in the future.

Log aggregation: Centralizes log data from multiple devices, making it easier to analyze and ensuring logs are available for future reference.

DLP (Data Loss Prevention): Focuses on preventing unauthorized data transfer and ensuring data security.

Archiving: Involves storing data for long-term retention, which could be part of log aggregation but is broader in scope.

SCAP (Security Content Automation Protocol): A standard for automating vulnerability management and policy compliance.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.4 - Explain security alerting and monitoring concepts and tools (Log aggregation).

199. Which of the following security concepts is being followed when implementing a product that offers protection against DDoS attacks?

- A. Availability
- B. Non-repudiation
- C. Integrity
- D. Confidentiality

Answer: A

Explanation:

When implementing a product that offers protection against Distributed Denial of Service (DDoS) attacks, the security concept being followed is availability. DDoS protection ensures that systems and services remain accessible to legitimate users even under attack, maintaining the availability of network resources.

Availability: Ensures that systems and services are accessible when needed, which is directly addressed by DDoS protection.

Non-repudiation: Ensures that actions or transactions cannot be denied by the involved parties, typically achieved through logging and digital signatures.

Integrity: Ensures that data is accurate and has not been tampered with.

Confidentiality: Ensures that information is accessible only to authorized individuals.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2 - Summarize fundamental security concepts (Availability).

200. A security analyst is reviewing the source code of an application in order to identify misconfigurations and vulnerabilities.

Which of the following kinds of analysis best describes this review?

- A. Dynamic
- B. Static
- C. Gap
- D. Impact

Answer: B

Explanation:

Reviewing the source code of an application to identify misconfigurations and vulnerabilities is best described as static analysis. Static analysis involves examining the code without executing the program. It focuses on finding potential security issues, coding errors, and vulnerabilities by analyzing the code itself.

Static analysis: Analyzes the source code or compiled code for vulnerabilities without executing the program.

Dynamic analysis: Involves testing and evaluating the program while it is running to identify vulnerabilities.

Gap analysis: Identifies differences between the current state and desired state, often used for compliance or process improvement.

Impact analysis: Assesses the potential effects of changes in a system or process.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.3 - Explain various activities associated with vulnerability management (Static analysis).

201. A company most likely is developing a critical system for the government and storing project information on a fileshare.

Which of the following describes how this data will be classified? (Select two).

- A. Private
- B. Confidential
- C. Public
- D. Operational
- E. Urgent

F. Restricted

Answer: B, F

Explanation:

When a company is developing a critical system for the government and storing project information on a fileshare, the data will most likely be classified as Confidential and Restricted.

Confidential: Indicates that the data is sensitive and access is limited to authorized individuals. This classification is typically used for information that could cause harm if disclosed.

Restricted: Indicates that access to the data is highly controlled and limited to those with a specific need to know. This classification is often used for highly sensitive information that requires stringent protection measures.

Private: Generally refers to personal information that is not meant to be publicly accessible.

Public: Information that is intended for public access and does not require protection.

Operational: Relates to day-to-day operations, but not necessarily to data classification.

Urgent: Refers to the priority of action rather than data classification.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1 - Security program management and oversight (Data classification).

202. Which of the following would be used to detect an employee who is emailing a customer list to a personal account before leaving the company?

A. DLP

B. FIM

C. IDS

D. EDR

Answer: A

Explanation:

To detect an employee who is emailing a customer list to a personal account before leaving the company, a Data Loss Prevention (DLP) system would be used. DLP systems are designed to detect and prevent unauthorized transmission of sensitive data.

DLP (Data Loss Prevention): Monitors and controls data transfers to ensure sensitive information is not sent to unauthorized recipients.

FIM (File Integrity Monitoring): Monitors changes to files to detect unauthorized modifications.

IDS (Intrusion Detection System): Monitors network traffic for suspicious activity but does not specifically prevent data leakage.

EDR (Endpoint Detection and Response): Monitors and responds to threats on endpoints but is not specifically focused on data leakage.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.5 - Modify enterprise capabilities to enhance security (Data Loss Prevention).

203. An engineer moved to another team and is unable to access the new team's shared folders while still being able to access the shared folders from the former team. After opening a ticket, the engineer discovers that the account was never moved to the new group.

Which of the following access controls is most likely causing the lack of access?

A. Role-based

B. Discretionary

- C. Time of day
- D. Least privilege

Answer: A

Explanation:

The most likely access control causing the lack of access is role-based access control (RBAC). In RBAC, access to resources is determined by the roles assigned to users. Since the engineer's account was not moved to the new group's role, the engineer does not have the necessary permissions to access the new team's shared folders.

Role-based access control (RBAC): Assigns permissions based on the user's role within the organization. If the engineer's role does not include the new group's permissions, access will be denied.

Discretionary access control (DAC): Access is based on the discretion of the data owner, but it is not typically related to group membership changes.

Time of day: Restricts access based on the time but does not affect group memberships.

Least privilege: Ensures users have the minimum necessary permissions, but the issue here is about group membership, not the principle of least privilege.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.6 - Implement and maintain identity and access management (Role-based access control).

204. Which of the following penetration testing teams is focused only on trying to compromise an organization using an attacker's tactics?

- A. White
- B. Red
- C. Purple
- D. Blue

Answer: B

Explanation:

Red teams are focused only on trying to compromise an organization using an attacker's tactics. They simulate real-world attacks to test the effectiveness of the organization's security defenses and identify vulnerabilities.

Red team: Acts as adversaries to simulate attacks and find security weaknesses.

White team: Oversees and ensures the rules of engagement are followed during the penetration test.

Purple team: Facilitates collaboration between the red team and the blue team to improve security.

Blue team: Defends against attacks and responds to security incidents.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.5 - Types and purposes of audits and assessments (Penetration testing: Red team).

205. A manager receives an email that contains a link to receive a refund. After hovering over the link, the manager notices that the domain's URL points to a suspicious link.

Which of the following security practices helped the manager to identify the attack?

- A. End user training
- B. Policy review
- C. URL scanning
- D. Plain text email

Answer: A

Explanation:

The security practice that helped the manager identify the suspicious link is end-user training. Training users to recognize phishing attempts and other social engineering attacks, such as hovering over links to check the actual URL, is a critical component of an organization's security awareness program.

End user training: Educates employees on how to identify and respond to security threats, including suspicious emails and phishing attempts.

Policy review: Ensures that policies are understood and followed but does not directly help in identifying specific attacks.

URL scanning: Automatically checks URLs for threats, but the manager identified the issue manually.

Plain text email: Ensures email content is readable without executing scripts, but the identification in this case was due to user awareness.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.6 - Implement security awareness practices (End-user training).

206. To improve the security at a data center, a security administrator implements a CCTV system and posts several signs about the possibility of being filmed.

Which of the following best describe these types of controls? (Select two).

- A. Preventive
- B. Deterrent
- C. Corrective
- D. Directive
- E. Compensating
- F. Detective

Answer: BF

Explanation:

The CCTV system and signs about the possibility of being filmed serve as both deterrent and detective controls.

Deterrent controls: Aim to discourage potential attackers from attempting unauthorized actions. Posting signs about CCTV serves as a deterrent by warning individuals that their actions are being monitored.

Detective controls: Identify and record unauthorized or suspicious activity. The CCTV system itself functions as a detective control by capturing and recording footage that can be reviewed later.

Preventive controls: Aim to prevent security incidents but are not directly addressed by the CCTV and signs in this context.

Corrective controls: Aim to correct or mitigate the impact of a security incident.

Directive controls: Provide guidelines or instructions but are not directly addressed by the CCTV and signs.

Compensating controls: Provide alternative measures to compensate for the absence or failure of primary controls.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1 - Compare and contrast various types of security controls (Deterrent and detective controls).

207. During a recent breach, employee credentials were compromised when a service desk employee issued an MFA bypass code to an attacker who called and posed as an employee.

Which of the following should be used to prevent this type of incident in the future?

- A. Hardware token MFA
- B. Biometrics
- C. Identity proofing
- D. Least privilege

Answer: C

Explanation:

To prevent the issuance of an MFA bypass code to an attacker posing as an employee, implementing identity proofing would be most effective. Identity proofing involves verifying the identity of individuals before granting access or providing sensitive information.

Identity proofing: Ensures that the person requesting the MFA bypass is who they claim to be, thereby preventing social engineering attacks where attackers pose as legitimate employees.

Hardware token MFA: Provides an additional factor for authentication but does not address verifying the requester's identity.

Biometrics: Offers strong authentication based on physical characteristics but is not related to the process of issuing MFA bypass codes.

Least privilege: Limits access rights for users to the bare minimum necessary to perform their work but does not prevent social engineering attacks targeting the service desk.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.6 - Implement and maintain identity and access management (Identity proofing).

208. The marketing department set up its own project management software without telling the appropriate departments.

Which of the following describes this scenario?

- A. Shadow IT
- B. Insider threat
- C. Data exfiltration
- D. Service disruption

Answer: A

Explanation:

The marketing department setting up its own project management software without informing the appropriate departments is an example of Shadow IT. Shadow IT refers to the use of IT systems, devices, software, applications, and services without explicit approval from the IT department.

Shadow IT: Involves the use of unauthorized systems and applications within an organization, which can lead to security risks and compliance issues.

Insider threat: Refers to threats from individuals within the organization who may intentionally cause harm or misuse their access, but this scenario is more about unauthorized use rather than malicious intent.

Data exfiltration: Involves unauthorized transfer of data out of the organization, which is not the main issue in this scenario.

Service disruption: Refers to interruptions in service availability, which is not directly related to the marketing department's actions.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 2.1 - Compare and contrast common threat actors and motivations (Shadow IT).

209. A network administrator is working on a project to deploy a load balancer in the company's cloud environment.

Which of the following fundamental security requirements does this project fulfill?

- A. Privacy
- B. Integrity
- C. Confidentiality
- D. Availability

Answer: D

Explanation:

Deploying a load balancer in the company's cloud environment primarily fulfills the fundamental security requirement of availability. A load balancer distributes incoming network traffic across multiple servers, ensuring that no single server becomes overwhelmed and that the service remains available even if some servers fail.

Availability: Ensures that services and resources are accessible when needed, which is directly supported by load balancing.

Privacy: Protects personal and sensitive information from unauthorized access but is not directly related to load balancing.

Integrity: Ensures that data is accurate and has not been tampered with, but load balancing is not primarily focused on data integrity.

Confidentiality: Ensures that information is accessible only to authorized individuals, which is not the primary concern of load balancing.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2 - Summarize fundamental security concepts (Availability).

210. A security engineer needs to configure an NGFW to minimize the impact of the increasing number of various traffic types during attacks.

Which of the following types of rules is the engineer the most likely to configure?

- A. Signature-based
- B. Behavioral-based
- C. URL-based
- D. Agent-based

Answer: B

Explanation:

To minimize the impact of the increasing number of various traffic types during attacks, a security engineer is most likely to configure behavioral-based rules on a Next-Generation Firewall (NGFW). Behavioral-based rules analyze the behavior of traffic patterns and can detect and block unusual or malicious activity that deviates from normal behavior.

Behavioral-based: Detects anomalies by comparing current traffic behavior to known good behavior, making it effective against various traffic types during attacks.

Signature-based: Relies on known patterns of known threats, which might not be as effective against new or varied attack types.

URL-based: Controls access to websites based on URL categories but is not specifically aimed at handling diverse traffic types during attacks.

Agent-based: Typically involves software agents on endpoints to monitor and enforce policies, not

directly related to NGFW rules.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.5 - Modify enterprise capabilities to enhance security (Behavioral-based rules on NGFW).

211. A security administrator identifies an application that is storing data using MD5.
Which of the following best identifies the vulnerability likely present in the application?

- A. Cryptographic
- B. Malicious update
- C. Zero day
- D. Side loading

Answer: A

Explanation:

The vulnerability likely present in the application that is storing data using MD5 is a cryptographic vulnerability. MD5 is considered to be a weak hashing algorithm due to its susceptibility to collision attacks, where two different inputs produce the same hash output, compromising data integrity and security.

Cryptographic: Refers to vulnerabilities in cryptographic algorithms or implementations, such as the weaknesses in MD5.

Malicious update: Refers to the intentional injection of harmful updates, not related to the use of MD5.

Zero day: Refers to previously unknown vulnerabilities for which no patch is available, not specifically related to MD5.

Side loading: Involves installing software from unofficial sources, not directly related to the use of MD5.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.4 - Explain the importance of using appropriate cryptographic solutions (MD5 vulnerabilities).

212. A company that is located in an area prone to hurricanes is developing a disaster recovery plan and looking at site considerations that allow the company to immediately continue operations.

Which of the following is the best type of site for this company?

- A. Cold
- B. Tertiary
- C. Warm
- D. Hot

Answer: D

Explanation:

For a company located in an area prone to hurricanes and needing to immediately continue operations, the best type of site is a hot site. A hot site is a fully operational offsite data center that is equipped with hardware, software, and network connectivity and is ready to take over operations with minimal downtime.

Hot site: Fully operational and can take over business operations almost immediately after a disaster.

Cold site: A basic site with infrastructure in place but without hardware or data, requiring significant time to become operational.

Tertiary site: Not a standard term in disaster recovery; it usually refers to an additional backup location but lacks the specifics of readiness.

Warm site: Equipped with hardware and connectivity but requires some time and effort to become fully

operational, not as immediate as a hot site.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 3.4 - Importance of resilience and recovery in security architecture (Site considerations: Hot site).

213. Which of the following security controls is most likely being used when a critical legacy server is segmented into a private network?

- A. Deterrent
- B. Corrective
- C. Compensating
- D. Preventive

Answer: C

Explanation:

When a critical legacy server is segmented into a private network, the security control being used is compensating. Compensating controls are alternative measures put in place to satisfy a security requirement when the primary control is not feasible or practical. In this case, segmenting the legacy server into a private network serves as a compensating control to protect it from potential vulnerabilities that cannot be mitigated directly.

Compensating: Provides an alternative method to achieve the desired security outcome when the primary control is not possible.

Deterrent: Aims to discourage potential attackers but does not directly address segmentation.

Corrective: Used to correct or mitigate the impact of an incident after it has occurred.

Preventive: Aims to prevent security incidents but is not specific to the context of segmentation.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1 - Compare and contrast various types of security controls (Compensating controls).

214. A company hired a security manager from outside the organization to lead security operations. Which of the following actions should the security manager perform first in this new role?

- A. Establish a security baseline.
- B. Review security policies.
- C. Adopt security benchmarks.
- D. Perform a user ID revalidation.

Answer: B

Explanation:

When a security manager is hired from outside the organization to lead security operations, the first action should be to review the existing security policies. Understanding the current security policies provides a foundation for identifying strengths, weaknesses, and areas that require improvement, ensuring that the security program aligns with the organization's goals and regulatory requirements. Review security policies: Provides a comprehensive understanding of the existing security framework, helping the new manager to identify gaps and areas for enhancement.

Establish a security baseline: Important but should be based on a thorough understanding of existing policies and practices.

Adopt security benchmarks: Useful for setting standards, but reviewing current policies is a necessary precursor.

Perform a user ID revalidation: Important for ensuring user access is appropriate but not the first step in

understanding overall security operations.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1 - Summarize elements of effective security governance (Reviewing security policies).

215. A company is decommissioning its physical servers and replacing them with an architecture that will reduce the number of individual operating systems.

Which of the following strategies should the company use to achieve this security requirement?

- A. Microservices
- B. Containerization
- C. Virtualization
- D. Infrastructure as code

Answer: C

Explanation:

To reduce the number of individual operating systems while decommissioning physical servers, the company should use containerization. Containerization allows multiple applications to run in isolated environments on a single operating system, significantly reducing the overhead compared to running multiple virtual machines, each with its own OS.

Containerization: Uses containers to run multiple isolated applications on a single OS kernel, reducing the need for multiple OS instances and improving resource utilization.

Microservices: An architectural style that structures an application as a collection of loosely coupled services, which does not necessarily reduce the number of operating systems.

Virtualization: Allows multiple virtual machines to run on a single physical server, but each VM requires its own OS, not reducing the number of OS instances.

Infrastructure as code: Manages and provisions computing infrastructure through machine-readable configuration files, but it does not directly impact the number of operating systems.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 3.1 - Compare and contrast security implications of different architecture models (Containerization).

216. An organization wants to ensure the integrity of compiled binaries in the production environment.

Which of the following security measures would best support this objective?

- A. Input validation
- B. Code signing
- C. SQL injection
- D. Static analysis

Answer: B

Explanation:

To ensure the integrity of compiled binaries in the production environment, the best security measure is code signing. Code signing uses digital signatures to verify the authenticity and integrity of the software, ensuring that the code has not been tampered with or altered after it was signed.

Code signing: Involves signing code with a digital signature to verify its authenticity and integrity, ensuring the compiled binaries have not been altered.

Input validation: Ensures that only properly formatted data enters an application but does not verify the integrity of compiled binaries.

SQL injection: A type of attack, not a security measure.

Static analysis: Analyzes code for vulnerabilities and errors but does not ensure the integrity of compiled binaries in production.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.4 - Explain the importance of using appropriate cryptographic solutions (Code signing).

217. A systems administrator would like to deploy a change to a production system.

Which of the following must the administrator submit to demonstrate that the system can be restored to a working state in the event of a performance issue?

- A. Backout plan
- B. Impact analysis
- C. Test procedure
- D. Approval procedure

Answer: A

Explanation:

To demonstrate that the system can be restored to a working state in the event of a performance issue after deploying a change, the systems administrator must submit a backout plan. A backout plan outlines the steps to revert the system to its previous state if the new deployment causes problems.

Backout plan: Provides detailed steps to revert changes and restore the system to its previous state in case of issues, ensuring minimal disruption and quick recovery.

Impact analysis: Evaluates the potential effects of a change but does not provide steps to revert changes.

Test procedure: Details the steps for testing the change but does not address restoring the system to a previous state.

Approval procedure: Involves obtaining permissions for the change but does not ensure system recovery in case of issues.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.3 - Explain the importance of change management processes (Backout plan).

218. A security administrator is configuring fileshares. The administrator removed the default permissions and added permissions for only users who will need to access the fileshares as part of their job duties.

Which of the following best describes why the administrator performed these actions?

- A. Encryption standard compliance
- B. Data replication requirements
- C. Least privilege
- D. Access control monitoring

Answer: C

Explanation:

The security administrator's actions of removing default permissions and adding permissions only for users who need access as part of their job duties best describe the principle of least privilege. This principle ensures that users are granted the minimum necessary access to perform their job functions, reducing the risk of unauthorized access or data breaches.

Least privilege: Limits access rights for users to the bare minimum necessary for their job duties, enhancing security by reducing potential attack surfaces.

Encryption standard compliance: Involves meeting encryption requirements, but it does not explain the

removal and assignment of specific permissions.

Data replication requirements: Focus on duplicating data across different systems for redundancy and availability, not related to user permissions.

Access control monitoring: Involves tracking and reviewing access to resources, but the scenario is about setting permissions, not monitoring them.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.5 - Modify enterprise capabilities to enhance security (Least privilege).

219. Which of the following describes effective change management procedures?

- A. Approving the change after a successful deployment
- B. Having a backout plan when a patch fails
- C. Using a spreadsheet for tracking changes
- D. Using an automatic change control bypass for security updates

Answer: B

Explanation:

Effective change management procedures include having a backout plan when a patch fails. A backout plan ensures that there are predefined steps to revert the system to its previous state if the new change or patch causes issues, thereby minimizing downtime and mitigating potential negative impacts.

Having a backout plan when a patch fails: Essential for ensuring that changes can be safely reverted in case of problems, maintaining system stability and availability.

Approving the change after a successful deployment: Changes should be approved before deployment, not after.

Using a spreadsheet for tracking changes: While useful for documentation, it is not a comprehensive change management procedure.

Using an automatic change control bypass for security updates: Bypassing change control can lead to unapproved and potentially disruptive changes.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.3 - Explain the importance of change management processes (Backout plan).

220. Which of the following tasks is typically included in the BIA process?

- A. Estimating the recovery time of systems
- B. Identifying the communication strategy
- C. Evaluating the risk management plan
- D. Establishing the backup and recovery procedures
- E. Developing the incident response plan

Answer: A

Explanation:

Estimating the recovery time of systems is a task typically included in the Business Impact Analysis (BIA) process. BIA involves identifying the critical functions of a business and determining the impact of a disruption. This includes estimating how long it will take to recover systems and resume normal operations.

Estimating the recovery time of systems: A key component of BIA, which helps in understanding the time needed to restore systems and services after a disruption.

Identifying the communication strategy: Typically part of the incident response plan, not BIA.

Evaluating the risk management plan: Part of risk management, not specifically BIA.

Establishing the backup and recovery procedures: Important for disaster recovery, not directly part of BIA.

Developing the incident response plan: Focuses on responding to security incidents, not on the impact analysis.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.2 - Risk management process (Business Impact Analysis - BIA).

221. An administrator needs to perform server hardening before deployment.

Which of the following steps should the administrator take? (Select two).

- A. Disable default accounts.
- B. Add the server to the asset inventory.
- C. Remove unnecessary services.
- D. Document default passwords.
- E. Send server logs to the SIEM.
- E. Join the server to the corporate domain.

Answer: A, C

Explanation:

To perform server hardening before deployment, the administrator should disable default accounts and remove unnecessary services. These steps are crucial to reducing the attack surface and enhancing the security of the server.

Disable default accounts: Default accounts often come with default credentials that are well-known and can be exploited by attackers. Disabling these accounts helps prevent unauthorized access.

Remove unnecessary services: Unnecessary services can introduce vulnerabilities and be exploited by attackers. Removing them reduces the number of potential attack vectors.

Add the server to the asset inventory: Important for tracking and management but not directly related to hardening.

Document default passwords: Documentation is useful, but changing or disabling default passwords is the hardening step.

Send server logs to the SIEM: Useful for monitoring and analysis but not a direct hardening step.

Join the server to the corporate domain: Part of integration into the network but not specific to hardening.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1 - Compare and contrast various types of security controls (Server hardening).

222. A company would like to provide employees with computers that do not have access to the internet in order to prevent information from being leaked to an online forum.

Which of the following would be best for the systems administrator to implement?

- A. Air gap
- B. Jump server
- C. Logical segmentation
- D. Virtualization

Answer: A

Explanation:

To provide employees with computers that do not have access to the internet and prevent information

leaks to an online forum, implementing an air gap would be the best solution. An air gap physically isolates the computer or network from any outside connections, including the internet, ensuring that data cannot be transferred to or from the system.

Air gap: A security measure that isolates a computer or network from the internet or other networks, preventing any form of electronic communication with external systems.

Jump server: A secure server used to access and manage devices in a different security zone, but it does not provide isolation from the internet.

Logical segmentation: Segregates networks using software or network configurations, but it does not guarantee complete isolation from the internet.

Virtualization: Creates virtual instances of systems, which can be isolated, but does not inherently prevent internet access without additional configurations.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5 - Explain the purpose of mitigation techniques used to secure the enterprise (Air gap).

223. Which of the following best describe a penetration test that resembles an actual external attack?

- A. Known environment
- B. Partially known environment
- C. Bug bounty
- D. Unknown environment

Answer: D

Explanation:

An unknown environment in penetration testing, also known as a black-box test, simulates an actual external attack where the tester has no prior knowledge of the system. This type of penetration test is designed to mimic real-world attack scenarios, where an attacker has little to no information about the target environment. The tester must rely on various reconnaissance and attack techniques to uncover vulnerabilities, much like a real-world attacker would. This approach helps organizations understand their security posture from an external perspective, providing insights into how their defenses would hold up against a true outsider threat.

Reference =

CompTIA Security+ SY0-701 Course Content: The course highlights the importance of understanding different penetration testing environments, including black-box testing, which aligns with the "unknown environment" in the provided answer.

CompTIA Security+ SY0-601 Study Guide: The guide details penetration testing methodologies, including black-box testing, which is crucial for simulating real external attacks.

224. A company is implementing a vendor's security tool in the cloud. The security director does not want to manage users and passwords specific to this tool but would rather utilize the company's standard user directory.

Which of the following should the company implement?

- A. 802.1X
- B. SAML
- C. RADIUS
- D. CHAP

Answer: B

Explanation:

The company should implement Security Assertion Markup Language (SAML) to integrate the vendor's security tool with their existing user directory. SAML is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP), enabling Single Sign-On (SSO). This allows the company to use its existing directory services for authentication, avoiding the need to manage a separate set of user credentials for the new tool.

Reference: CompTIA Security+ SY0-701 Course Content: Domain 4: Identity and Access Management, which includes SAML as a key identity federation standard for SSO.

CompTIA Security+ Study Guide (SY0-601): Chapter 8, "Identity and Access Management," details the role of SAML in enabling SSO by utilizing an existing identity provider.

225. An employee fell for a phishing scam, which allowed an attacker to gain access to a company PC. The attacker scraped the PC's memory to find other credentials. Without cracking these credentials, the attacker used them to move laterally through the corporate network.

Which of the following describes this type of attack?

- A. Privilege escalation
- B. Buffer overflow
- C. SQL injection
- D. Pass-the-hash

Answer: D

Explanation:

The scenario describes an attacker who obtained credentials from a compromised system's memory and used them without cracking to move laterally within the network. This technique is known as a "pass-the-hash" attack, where the attacker captures hashed credentials (e.g., NTLM hashes) and uses them to authenticate and gain access to other systems without needing to know the plaintext password. This is a common attack method in environments where weak security practices or outdated protocols are in use.

Reference =

CompTIA Security+ SY0-701 Course Content: The course discusses credential-based attacks like pass-the-hash, emphasizing their impact and the importance of protecting credential stores.

226. A company wants to reduce the time and expense associated with code deployment.

Which of the following technologies should the company utilize?

- A. Serverless architecture
- B. Thin clients
- C. Private cloud
- D. Virtual machines

Answer: A

Explanation:

Serverless architecture allows companies to deploy code without managing the underlying infrastructure. This approach significantly reduces the time and expense involved in code deployment because developers can focus solely on writing code, while the cloud provider manages the servers, scaling, and maintenance. Serverless computing also enables automatic scaling and pay-per-execution billing, which further optimizes costs.

Reference =

CompTIA Security+ SY0-701 Course Content: The course covers cloud technologies, including serverless architectures, which are highlighted as a method to streamline and reduce costs associated with code deployment.

227. A security team created a document that details the order in which critical systems should be brought back online after a major outage.

Which of the following documents did the team create?

- A. Communication plan
- B. Incident response plan
- C. Data retention policy
- D. Disaster recovery plan

Answer: D

Explanation:

The document described in the question is a Disaster Recovery Plan (DRP). A DRP outlines the process and procedures for restoring critical systems and operations after a major disruption or outage. It includes the order in which systems should be brought back online to ensure minimal impact on business operations, prioritizing the most critical systems to recover first.

Reference: CompTIA Security+ SY0-701 Course Content: Domain 5: Security Program Management and Oversight, which discusses the development and implementation of disaster recovery plans.

228. Which of the following best represents an application that does not have an on-premises requirement and is accessible from anywhere?

- A. Pass
- B. Hybrid cloud
- C. Private cloud
- D. IaaS
- E. SaaS

Answer: E

Explanation:

Software as a Service (SaaS) represents an application that is hosted in the cloud and accessible via the internet from anywhere, with no requirement for on-premises infrastructure. SaaS applications are managed by a third-party provider, allowing users to access them through a web browser, making them highly scalable and flexible for remote access.

Reference: CompTIA Security+ SY0-701 Course Content: Domain 3: Security Architecture, where cloud service models such as SaaS are discussed, highlighting their accessibility and lack of on-premises requirements.

229. A company is utilizing an offshore team to help support the finance department. The company wants to keep the data secure by keeping it on a company device but does not want to provide equipment to the offshore team.

Which of the following should the company implement to meet this requirement?

- A. VDI
- B. MDM
- C. VPN

D. VPC

Answer: A

Explanation:

Virtual Desktop Infrastructure (VDI) allows a company to host desktop environments on a centralized server. Offshore teams can access these virtual desktops remotely, ensuring that sensitive data stays within the company's infrastructure without the need to provide physical devices to the team. This solution is ideal for maintaining data security while enabling remote work, as all data processing occurs on the company's secure servers.

Reference =

CompTIA Security+ SY0-701 Course Content: VDI is discussed as a method for securely managing remote access to company resources without compromising data security.

230. The application development teams have been asked to answer the following questions:

- Does this application receive patches from an external source?
- Does this application contain open-source code?
- is this application accessible by external users?
- Does this application meet the corporate password standard?

Which of the following are these questions port of?

- A. Risk control self-assessment
- B. Risk management strategy
- C. Risk acceptance
- D. Risk matrix

Answer: A

Explanation:

The questions listed are part of a Risk Control Self-Assessment (RCSA), which is a process where teams evaluate the risks associated with their operations and assess the effectiveness of existing controls. The questions focus on aspects such as patch management, the use of open-source code, external access, and compliance with corporate standards, all of which are critical for identifying and mitigating risks.

Reference =

CompTIA Security+ SY0-701 Course Content: The course discusses various risk management processes, including self-assessments that help in identifying and managing risks within the organization.

231. An administrator is Investigating an incident and discovers several users' computers were Infected with malware after viewing files mat were shared with them. The administrator discovers no degraded performance in the infected machines and an examination of the log files does not show excessive failed logins.

Which of the following attacks Is most likely the cause of the malware?

- A. Malicious flash drive
- B. Remote access Trojan
- C. Brute-forced password
- D. Cryptojacking

Answer: D

Explanation:

Cryptojacking is the likely cause in this scenario. It involves malware that hijacks the resources of infected computers to mine cryptocurrency, usually without the user's knowledge. This type of attack doesn't typically degrade performance significantly or result in obvious system failures, which matches the situation described, where the machines showed no signs of degraded performance or excessive failed logins.

Reference =

CompTIA Security+ SY0-701 Course Content: Cryptojacking is covered under types of malware attacks, highlighting its stealthy nature and impact on infected systems.

232. Which of the following is an algorithm performed to verify that data has not been modified?

- A. Hash
- B. Code check
- C. Encryption
- D. Checksum

Answer: A

Explanation:

A hash is an algorithm used to verify data integrity by generating a fixed-size string of characters from input data. If even a single bit of the input data changes, the hash value will change, allowing users to detect any modification to the data. Hashing algorithms like SHA-256 and MD5 are commonly used to ensure data has not been altered.

Reference: CompTIA Security+ SY0-701 Course Content: Domain 6: Cryptography and PKI, which discusses the role of hashing in verifying data integrity.

233. An employee recently resigned from a company. The employee was responsible for managing and supporting weekly batch jobs over the past five years. A few weeks after the employee resigned, one of the batch jobs failed and caused a major disruption.

Which of the following would work best to prevent this type of incident from reoccurring?

- A. Job rotation
- B. Retention
- C. Outsourcing
- D. Separation of duties

Answer: A

Explanation:

Job rotation is a security control that involves regularly moving employees to different roles within an organization. This practice helps prevent incidents where a single employee has too much control or knowledge about a specific job function, reducing the risk of disruption when an employee leaves. It also helps in identifying any hidden issues or undocumented processes that could cause problems after an employee's departure.

Reference: CompTIA Security+ SY0-701 Course Content: Domain 5: Security Program Management and Oversight, which includes job rotation as a method to ensure business continuity and reduce risks.

234. A security manager is implementing MFA and patch management.

Which of the following would best describe the control type and category? (Select two).

- A. Physical
- B. Managerial
- C. Detective
- D. Administrator
- E. Preventative
- F. Technical

Answer: E, F

Explanation:

Multi-Factor Authentication (MFA) and patch management are both examples of preventative and technical controls. MFA prevents unauthorized access by requiring multiple forms of verification, and patch management ensures that systems are protected against vulnerabilities by applying updates. Both of these controls are implemented using technical methods, and they work to prevent security incidents before they occur.

Reference: CompTIA Security+ SY0-701 Course Content: Domain 1: General Security Concepts, and Domain 4: Identity and Access Management, which cover the implementation of preventative and technical controls.

235. An organization implemented cloud-managed IP cameras to monitor building entry points and sensitive areas. The service provider enables direct TCP/IP connection to stream live video footage from each camera. The organization wants to ensure this stream is encrypted and authenticated.

Which of the following protocols should be implemented to best meet this objective?

- A. SSH
- B. SRTP
- C. S/MIME
- D. PPTP

Answer: B

Explanation:

Secure Real-Time Transport Protocol (SRTP) is a security protocol used to encrypt and authenticate the streaming of audio and video over IP networks. It ensures that the video streams from the IP cameras are both encrypted to prevent unauthorized access and authenticated to verify the integrity of the stream, making it the ideal choice for securing video surveillance.

Reference: CompTIA Security+ SY0-701 Course Content: Domain 3: Security Architecture, which includes secure communication protocols like SRTP for protecting data in transit.

236. A security analyst discovers that a large number of employee credentials had been stolen and were being sold on the dark web. The analyst investigates and discovers that some hourly employee credentials were compromised, but salaried employee credentials were not affected.

Most employees clocked in and out while they were Inside the building using one of the kiosks connected to the network. However, some clocked out and recorded their time after leaving to go home. Only those who clocked in and out while Inside the building had credentials stolen. Each of the kiosks are on different floors, and there are multiple routers, since the business segments environments for certain business functions.

Hourly employees are required to use a website called acmetimekeeping.com to clock in and out. This website is accessible from the internet.

Which of the following is the most likely reason for this compromise?

- A. A brute-force attack was used against the time-keeping website to scan for common passwords.
- B. A malicious actor compromised the time-keeping website with malicious code using an unpatched vulnerability on the site, stealing the credentials.
- C. The internal DNS servers were poisoned and were redirecting acmetimkeeping.com to malicious domain that intercepted the credentials and then passed them through to the real site
- D. ARP poisoning affected the machines in the building and caused the kiosks to send a copy of all the submitted credentials to a machine.

Answer: B

Explanation:

The scenario suggests that only the employees who used the kiosks inside the building had their credentials compromised. Since the time-keeping website is accessible from the internet, it is possible that a malicious actor exploited an unpatched vulnerability in the site, allowing them to inject malicious code that captured the credentials of those who logged in from the kiosks. This is a common attack vector for stealing credentials from web applications.

Reference =

CompTIA Security+ SY0-701 Course Content: The course discusses web application vulnerabilities and how attackers can exploit them to steal credentials.

237. A business uses Wi-Fi with content filtering enabled. An employee noticed a coworker accessed a blocked site from a work computer and reported the issue. While investigating the issue, a security administrator found another device providing internet access to certain employees.

Which of the following best describes the security risk?

- A. The host-based security agent is not running on all computers.
- B. A rogue access point is allowing users to bypass controls.
- C. Employees who have certain credentials are using a hidden SSID.
- D. A valid access point is being jammed to limit availability.

Answer: B

Explanation:

The presence of another device providing internet access that bypasses the content filtering system indicates the existence of a rogue access point. Rogue access points are unauthorized devices that can create a backdoor into the network, allowing users to bypass security controls like content filtering. This presents a significant security risk as it can expose the network to unauthorized access and potential data breaches.

Reference =

CompTIA Security+ SY0-701 Course Content: Rogue access points are highlighted as a major security risk, allowing unauthorized access to the network and bypassing security measures.

238. Which of the following is most likely associated with introducing vulnerabilities on a corporate network by the deployment of unapproved software?

- A. Hacktivists
- B. Script kiddies
- C. Competitors

D. Shadow IT

Answer: D

Explanation:

Shadow IT refers to the use of information technology systems, devices, software, applications, and services without explicit IT department approval. This is the most likely cause of introducing vulnerabilities on a corporate network by deploying unapproved software, as such software may not have been vetted for security compliance, increasing the risk of vulnerabilities.

Reference =

CompTIA Security+ SY0-701 Course Content: The concept of Shadow IT is discussed as a significant risk due to the introduction of unapproved and potentially vulnerable software into the corporate network.

239. Two companies are in the process of merging. The companies need to decide how to standardize their information security programs.

Which of the following would best align the security programs?

- A. Shared deployment of CIS baselines
- B. Joint cybersecurity best practices
- C. Both companies following the same CSF
- D. Assessment of controls in a vulnerability report

Answer: C

Explanation:

A Cybersecurity Framework (CSF) provides a structured approach to standardizing and aligning security programs across different organizations. By both companies adopting the same CSF, they can ensure that their security measures, policies, and practices are consistent, which is essential during a merger when aligning two different security programs.

Reference =

CompTIA Security+ SY0-701 Course Content: The course discusses the importance of adopting standardized cybersecurity frameworks (CSF) for aligning security programs during mergers and acquisitions.

240. A network administrator deployed a DNS logging tool that logs suspicious websites that are visited and then sends a daily report based on various weighted metrics.

Which of the following best describes the type of control the administrator put in place?

- A. Preventive
- B. Deterrent
- C. Corrective
- D. Detective

Answer: D

Explanation:

The tool that the network administrator deployed is described as one that logs suspicious websites and sends a daily report based on various weighted metrics. This fits the description of a detective control. Detective controls are designed to identify and log security events or incidents after they have occurred. By analyzing these logs and generating reports, the tool helps in detecting potential security breaches, thus allowing for further investigation and response.

Reference = Based on the CompTIA Security+ SY0-701 Resources, specifically under the domain of

Security Operations, which discusses different types of security controls, including detective controls.

241.Which of the following is best used to detect fraud by assigning employees to different roles?

- A. Least privilege
- B. Mandatory vacation
- C. Separation of duties
- D. Job rotation

Answer: D

Explanation:

Job rotation is a strategy used in organizations to detect and prevent fraud by periodically assigning employees to different roles within the organization. This approach helps ensure that no single employee has exclusive control over a specific process or set of tasks for an extended period, thereby reducing the opportunity for fraudulent activities to go unnoticed. By rotating roles, organizations can uncover irregularities and discrepancies that might have been concealed by an employee who had prolonged access to sensitive functions. Job rotation also promotes cross-training, which can enhance the organization's overall resilience and flexibility.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
CompTIA Security+ SY0-601 Study Guide: Chapter on Risk Management and Compliance.

242.A systems administrator wants to implement a backup solution. the solution needs to allow recovery of the entire system, including the operating system, in case of a disaster.

Which of the following backup types should the administrator consider?

- A. Incremental
- B. Storage area network
- C. Differential
- D. Image

Answer: D

Explanation:

An image backup, also known as a full system backup, captures the entire contents of a system, including the operating system, applications, settings, and all data. This type of backup allows for a complete recovery of the system in case of a disaster, as it includes everything needed to restore the system to its previous state. This makes it the ideal choice for a systems administrator who needs to ensure the ability to recover the entire system, including the OS.

Reference = CompTIA Security+ SY0-701 study materials, domain on Security Operations.

243.A spoofed identity was detected for a digital certificate.

Which of the following are the type of unidentified key and the certificate that could be in use on the company domain?

- A. Private key and root certificate
- B. Public key and expired certificate
- C. Private key and self-signed certificate
- D. Public key and wildcard certificate

Answer: C

Explanation:

A self-signed certificate is a certificate that is signed by its own private key rather than by a trusted certificate authority (CA). This means that the authenticity of the certificate relies solely on the issuer's own authority. If a spoofed identity was detected, it could indicate that a private key associated with a self-signed certificate was compromised. Self-signed certificates are often used internally within organizations, but they carry higher risks since they are not validated by a third-party CA, making them more susceptible to spoofing.

Reference = CompTIA Security+ SY0-701 study materials, particularly the domains discussing Public Key Infrastructure (PKI) and certificate management.

244. The Chief Information Security Officer wants to put security measures in place to protect PII. The organization needs to use its existing labeling and classification system to accomplish this goal. Which of the following would most likely be configured to meet the requirements?

- A. Tokenization
- B. S/MIME
- C. DLP
- D. MFA

Answer: C

Explanation:

Data Loss Prevention (DLP) systems are typically configured to protect sensitive data such as Personally Identifiable Information (PII) within an organization. DLP tools enforce policies that monitor, detect, and block the unauthorized transmission of sensitive data. By leveraging the organization's existing labeling and classification system, DLP solutions can identify and protect data based on its classification, ensuring that PII is appropriately secured according to organizational policies.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Network Security and DLP.

245. An analyst is reviewing an incident in which a user clicked on a link in a phishing email. Which of the following log sources would the analyst utilize to determine whether the connection was successful?

- A. Network
- B. System
- C. Application
- D. Authentication

Answer: A

Explanation:

To determine whether the connection was successful after a user clicked on a link in a phishing email, the most relevant log source to analyze would be the network logs. These logs would provide information on outbound and inbound traffic, allowing the analyst to see if the user's system connected to the remote server specified in the phishing link. Network logs can include details such as IP addresses, domains accessed, and the success or failure of connections, which are crucial for understanding the impact of the phishing attempt.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Incident Response.

246. The Cruel Information Security Officer (CISO) asks a security analyst to install an OS update to a production VM that has a 99% uptime SL

A. The CISO tells me analyst the installation must be done as quickly as possible.

Which of the following courses of action should the security analyst take first?

A. Log in to the server and perform a health check on the VM.

B. Install the patch Immediately.

C. Confirm that the backup service is running.

D. Take a snapshot of the VM.

Answer: D

Explanation:

Before applying any updates or patches to a production VM, especially one with a 99% uptime SLA, it is crucial to first take a snapshot of the VM. This snapshot serves as a backup that can be quickly restored in case the update causes any issues, ensuring that the system can be returned to its previous state without violating the SLA. This step mitigates risk and is a standard best practice in change management for critical systems.

Reference = CompTIA Security+ SY0-701 study materials, focusing on change management and backup strategies.

247. Since a recent upgrade of a WLAN infrastructure, several mobile users have been unable to access the internet from the lobby. The networking team performs a heat map survey of the building and finds several WAPs in the area. The WAPs are using similar frequencies with high power settings.

Which of the following installation considerations should the security team evaluate next?

A. Channel overlap

B. Encryption type

C. New WLAN deployment

D. WAP placement

Answer: A

Explanation:

When multiple Wireless Access Points (WAPs) are using similar frequencies with high power settings, it can cause channel overlap, leading to interference and connectivity issues. This is likely the reason why mobile users are unable to access the internet in the lobby. Evaluating and adjusting the channel settings on the WAPs to avoid overlap is crucial to resolving the connectivity problems.

Reference = CompTIA Security+ SY0-701 study materials, particularly the domain on Wireless and Mobile Security, which covers WLAN deployment considerations.

248. An employee in the accounting department receives an email containing a demand for payment for services performed by a vendor. However, the vendor is not in the vendor management database.

Which of the following in this scenario is an example of?

A. Pretexting

B. Impersonation

C. Ransomware

D. Invoice scam

Answer: D

Explanation:

The scenario describes an instance where an employee receives a fraudulent invoice from a vendor that is not recognized in the company's vendor management system. This is a classic example of an invoice scam, where attackers attempt to trick organizations into making payments for fake or non-existent services. These scams often rely on social engineering tactics to bypass financial controls.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the context of social engineering attacks and common scams.

249. While considering the organization's cloud-adoption strategy, the Chief Information Security Officer sets a goal to outsource patching of firmware, operating systems, and applications to the chosen cloud vendor.

Which of the following best meets this goal?

- A. Community cloud
- B. PaaS
- C. Containerization
- D. Private cloud
- E. SaaS
- F. IaaS

Answer: E

Explanation:

Software as a Service (SaaS) is the cloud model that best meets the goal of outsourcing the management, including patching, of firmware, operating systems, and applications to the cloud vendor. In a SaaS environment, the cloud provider is responsible for maintaining and updating the entire software stack, allowing the organization to focus on using the software rather than managing its infrastructure.

Reference = CompTIA Security+ SY0-701 study materials, particularly the domains related to cloud security models.

250. A security analyst is assessing several company firewalls.

Which of the following tools would the analyst most likely use to generate custom packets to use during the assessment?

- A. hping
- B. Wireshark
- C. PowerShell
- D. netstat

Answer: A

Explanation:

Monitoring outbound traffic is essential for detecting unauthorized data exfiltration from a system. A new vulnerability that allows malware to move data unauthorizedly would typically attempt to send this data out of the network. By monitoring outbound traffic, security tools can detect unusual data transfers, trigger alerts, and help prevent the exfiltration of sensitive information.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Threat Detection and Response.

251. A new vulnerability enables a type of malware that allows the unauthorized movement of data from a system.

Which of the following would detect this behavior?

- A. Implementing encryption
- B. Monitoring outbound traffic
- C. Using default settings
- D. Closing all open ports

Answer: B

Explanation:

Monitoring outbound traffic is essential for detecting unauthorized data exfiltration from a system. A new vulnerability that allows malware to move data unauthorizedly would typically attempt to send this data out of the network. By monitoring outbound traffic, security tools can detect unusual data transfers, trigger alerts, and help prevent the exfiltration of sensitive information.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Threat Detection and Response.

252. Which of the following can a security director use to prioritize vulnerability patching within a company's IT environment?

- A. SOAR
- B. CVSS
- C. SIEM
- D. CVE

Answer: B

Explanation:

The Common Vulnerability Scoring System (CVSS) is a standardized framework for assessing the severity of security vulnerabilities. It helps organizations prioritize vulnerability patching by providing a numerical score that reflects the potential impact and exploitability of a vulnerability. CVSS scores are used to gauge the urgency of patching vulnerabilities within a company's IT environment.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.

CompTIA Security+ SY0-601 Study Guide: Chapter on Vulnerability Management.

253. Which of the following is the most effective way to protect an application server running software that is no longer supported from network threats?

- A. Air gap
- B. Barricade
- C. Port security
- D. Screen subnet

Answer: A

Explanation:

Air-gapping is the most effective way to protect an application server running unsupported software from network threats. By physically isolating the server from any network connection (no wired or wireless communication), it is protected from external cyber threats. While other options like port security or a screened subnet can provide some level of protection, an air gap offers the highest level of security by preventing any network-based attacks entirely.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Secure System Design.

254. Which of the following is the most important security concern when using legacy systems to provide production service?

- A. Instability
- B. Lack of vendor support
- C. Loss of availability
- D. Use of insecure protocols

Answer: B

Explanation:

The most important security concern when using legacy systems is the lack of vendor support. Without support from the vendor, systems may not receive critical security patches and updates, leaving them vulnerable to exploitation. This lack of support can result in increased risk of security breaches, as vulnerabilities discovered in the software may never be addressed.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the context of risk management and the challenges posed by legacy systems.

255. Cadets speaking a foreign language are using company phone numbers to make unsolicited phone calls to a partner organization. A security analyst validates through phone system logs that the calls are occurring and the numbers are not being spoofed.

Which of the following is the most likely explanation?

- A. The executive team is traveling internationally and trying to avoid roaming charges
- B. The company's SIP server security settings are weak.
- C. Disgruntled employees are making calls to the partner organization.
- D. The service provider has assigned multiple companies the same numbers

Answer: B

Explanation:

If cadets are using company phone numbers to make unsolicited calls, and the logs confirm the numbers are not being spoofed, it suggests that the SIP (Session Initiation Protocol) server's security settings might be weak. This could allow unauthorized access or exploitation of the company's telephony services, potentially leading to misuse by unauthorized individuals.

Reference = CompTIA Security+ SY0-701 study materials, especially on SIP security and common vulnerabilities.

256. An IT security team is concerned about the confidentiality of documents left unattended in MFPs. Which of the following should the security team do to mitigate the situation?

- A. Educate users about the importance of paper shredder devices.

- B. Deploy an authentication factor that requires In-person action before printing.
- C. Install a software client on every computer authorized to use the MFPs.
- D. Update the management software to utilize encryption.

Answer: B

Explanation:

To mitigate the risk of confidential documents being left unattended in Multi-Function Printers (MFPs), implementing an authentication factor that requires in-person action before printing (such as PIN codes or badge scanning) is the most effective measure. This ensures that documents are only printed when the authorized user is present to collect them, reducing the risk of sensitive information being exposed. Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of physical security and access control.

257. A systems administrator is auditing all company servers to ensure they meet the minimum security baseline. While auditing a Linux server, the systems administrator observes the `/etc/shadow` file has permissions beyond the baseline recommendation.

Which of the following commands should the systems administrator use to resolve this issue?

- A. `chmod`
- B. `grep`
- C. `dd`
- D. `passwd`

Answer: A

Explanation:

The `chmod` command is used to change file permissions on Unix and Linux systems. If the `/etc/shadow` file has permissions beyond the baseline recommendation, the systems administrator should use `chmod` to modify the file's permissions, ensuring it adheres to the security baseline and limits access to authorized users only.

Reference = CompTIA Security+ SY0-701 study materials, focusing on system hardening and file permissions management.

258. During a recent company safety stand-down, the cyber-awareness team gave a presentation on the importance of cyber hygiene. One topic the team covered was best practices for printing centers.

Which of the following describes an attack method that relates to printing centers?

- A. Whaling
- B. Credential harvesting
- C. Prepending
- D. Dumpster diving

Answer: D

Explanation:

Dumpster diving is an attack method where attackers search through physical waste, such as discarded documents and printouts, to find sensitive information that has not been properly disposed of. In the context of printing centers, this could involve attackers retrieving printed documents containing confidential data that were improperly discarded without shredding or other secure disposal methods. This emphasizes the importance of proper disposal and physical security measures in cyber hygiene practices.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Physical Security and Cyber Hygiene.

259. A software developer would like to ensure. The source code cannot be reverse engineered or debugged.

Which of the following should the developer consider?

- A. Version control
- B. Obfuscation toolkit
- C. Code reuse
- D. Continuous integration
- E. Stored procedures

Answer: B

Explanation:

An obfuscation toolkit is used by developers to make source code difficult to understand and reverse engineer. This technique involves altering the code's structure and naming conventions without changing its functionality, making it much harder for attackers to decipher the code or use debugging tools to analyze it. Obfuscation is an important practice in protecting proprietary software and intellectual property from reverse engineering.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Secure Coding Practices.

260. Which of the following is a common source of unintentional corporate credential leakage in cloud environments?

- A. Code repositories
- B. Dark web
- C. Threat feeds
- D. State actors
- E. Vulnerability databases

Answer: A

Explanation:

Code repositories are a common source of unintentional corporate credential leakage, especially in cloud environments. Developers may accidentally commit and push sensitive information, such as API keys, passwords, and other credentials, to public or poorly secured repositories. These credentials can then be accessed by unauthorized users, leading to security breaches. Ensuring that repositories are properly secured and that sensitive data is never committed is critical for protecting against this type of leakage.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Threats and Vulnerability Management.

261. A security audit of an organization revealed that most of the IT staff members have domain administrator credentials and do not change the passwords regularly.

Which of the following solutions should the security team propose to resolve the findings in the most complete way?

- A. Creating group policies to enforce password rotation on domain administrator credentials
- B. Reviewing the domain administrator group, removing all unnecessary administrators, and rotating all passwords
- C. Integrating the domain administrator's group with an IdP and requiring SSO with MFA for all access
- D. Securing domain administrator credentials in a PAM vault and controlling access with role-based access control

Answer: D

Explanation:

Using a Privileged Access Management (PAM) vault to secure domain administrator credentials and enforcing role-based access control (RBAC) is the most comprehensive solution. PAM systems help manage and control access to privileged accounts, ensuring that only authorized personnel can access sensitive credentials. This approach also facilitates password rotation, auditing, and ensures that credentials are not misused or left unchanged. Integrating PAM with RBAC ensures that access is granted based on the user's role, further enhancing security.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

262. A company wants to get alerts when others are researching and doing reconnaissance on the company. One approach would be to host a part of the Infrastructure online with known vulnerabilities that would appear to be company assets.

Which of the following describes this approach?

- A. Watering hole
- B. Bug bounty
- C. DNS sinkhole
- D. Honeypot

Answer: D

Explanation:

A honeypot is a security mechanism set up to attract and detect potential attackers by simulating vulnerable assets. By hosting a part of the infrastructure online with known vulnerabilities that appear to be company assets, the company can observe and analyze the behavior of attackers conducting reconnaissance. This approach allows the company to get alerts and gather intelligence on potential threats.

Reference = CompTIA Security+ SY0-701 study materials, particularly on threat detection techniques such as honeypots.

263. Which of the following best describes why the SMS OTP authentication method is more risky to implement than the TOTP method?

- A. The SMS OTP method requires an end user to have an active mobile telephone service and SIM card.
- B. Generally, SMS OTP codes are valid for up to 15 minutes while the TOTP time frame is 30 to 60 seconds

C. The SMS OTP is more likely to be intercepted and lead to unauthorized disclosure of the code than the TOTP method.

D. The algorithm used to generate on SMS OTP code is weaker than the one used to generate a TOTP code

Answer: C

Explanation:

The SMS OTP (One-Time Password) method is more vulnerable to interception compared to TOTP (Time-based One-Time Password) because SMS messages can be intercepted through various attack vectors like SIM swapping or SMS phishing. TOTP, on the other hand, generates codes directly on the device and does not rely on a communication channel like SMS, making it less susceptible to interception.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management.

264. A website user is locked out of an account after clicking an email link and visiting a different website. Web server logs show the user's password was changed, even though the user did not change the password.

Which of the following is the most likely cause?

A. Cross-site request forgery

B. Directory traversal

C. ARP poisoning

D. SQL injection

Answer: A

Explanation:

The scenario describes a situation where a user unknowingly triggers an unwanted action, such as changing their password, by clicking a malicious link. This is indicative of a Cross-Site Request Forgery (CSRF) attack, where an attacker tricks the user into executing actions they did not intend to perform on a web application in which they are authenticated.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of web application security and common attack vectors like CSRF.

265. A security engineer is working to address the growing risks that shadow IT services are introducing to the organization. The organization has taken a cloud-first approach and does not have an on-premises IT infrastructure.

Which of the following would best secure the organization?

A. Upgrading to a next-generation firewall

B. Deploying an appropriate in-line CASB solution

C. Conducting user training on software policies

D. Configuring double key encryption in SaaS platforms

Answer: B

Explanation:

A Cloud Access Security Broker (CASB) solution is the most suitable option for securing an organization that has adopted a cloud-first strategy and does not have an on-premises IT infrastructure. CASBs provide visibility and control over shadow IT services, enforce security policies, and protect data across

cloud services.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of cloud security and managing risks associated with shadow IT.

266. A cybersecurity incident response team at a large company receives notification that malware is present on several corporate desktops. No known Indicators of compromise have been found on the network.

Which of the following should the team do first to secure the environment?

- A. Contain the Impacted hosts
- B. Add the malware to the application blocklist.
- C. Segment the core database server.
- D. Implement firewall rules to block outbound beaconing

Answer: A

Explanation:

The first step in responding to a cybersecurity incident, particularly when malware is detected, is to contain the impacted hosts. This action prevents the spread of malware to other parts of the network, limiting the potential damage while further investigation and remediation actions are planned.

Reference = CompTIA Security+ SY0-701 study materials, particularly on incident response procedures and the importance of containment in managing security incidents.

267. Which of the following is a reason why a forensic specialist would create a plan to preserve data after an incident and prioritize the sequence for performing forensic analysis?

- A. Order of volatility
- B. Preservation of event logs
- C. Chain of custody
- D. Compliance with legal hold

Answer: A

Explanation:

When conducting a forensic analysis after an incident, it's essential to prioritize the data collection process based on the "order of volatility." This principle dictates that more volatile data (e.g., data in memory, network connections) should be captured before less volatile data (e.g., disk drives, logs). The idea is to preserve the most transient and potentially valuable evidence first, as it is more likely to be lost or altered quickly.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Digital Forensics.

268. A security analyst is creating a base for the server team to follow when hardening new devices for deployment.

Which of the following best describes what the analyst is creating?

- A. Change management procedure
- B. Information security policy
- C. Cybersecurity framework
- D. Secure configuration guide

Answer: D

Explanation:

The security analyst is creating a "secure configuration guide," which is a set of instructions or guidelines used to configure devices securely before deployment. This guide ensures that the devices are set up according to best practices to minimize vulnerabilities and protect against potential security threats.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on System Hardening and Secure Configuration.

269. In which of the following scenarios is tokenization the best privacy technique to use?

- A. Providing pseudo-anonymization for social media user accounts
- B. Serving as a second factor for authentication requests
- C. Enabling established customers to safely store credit card information
- D. Masking personal information inside databases by segmenting data

Answer: C

Explanation:

Tokenization is a process that replaces sensitive data, such as credit card information, with a non-sensitive equivalent (token) that can be used in place of the actual data. This technique is particularly useful in securely storing payment information because the token can be safely stored and transmitted without exposing the original credit card number.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptography and Data Protection.

270. A security administrator recently reset local passwords and the following values were recorded in the system:

Host	Account	MD5 password values
ACCT-PC-1	admin	f1bdf5ed1d7ad7ede4e3809bd35644b0
HR-PC-1	admin	d706ab8258fe67c131ebc57a6e28184
IT-PC-2	admin	f8ddb9cbb321d7dfbf6cb059736f0b3d
FILE-SRV-1	admin	f054bbd2f5ebab9cb5571006b2c60c02
DB-SRV-1	admin	8638f732ba7cf2d95b16979e2725da78

Which of the following is the security administrator most likely protecting against?

- A. Account sharing
- B. Weak password complexity
- C. Pass-the-hash attacks
- D. Password compromise

Answer: C

Explanation:

The scenario shows MD5 hashed password values. The most likely reason the security administrator is focusing on these values is to protect against pass-the-hash attacks. In this type of attack, an attacker can use a captured hash to authenticate without needing to know the actual plaintext password. By managing and monitoring these hashes, the administrator can implement strategies to mitigate this type of threat.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

271. A vendor needs to remotely and securely transfer files from one server to another using the command line.

Which of the following protocols should be Implemented to allow for this type of access? (Select two).

- A. SSH
- B. SNMP
- C. RDP
- D. S/MIME
- E. SMTP
- F. SFTP

Answer: A, F

Explanation:

Secure Shell (SSH) is a protocol used for secure command-line access to remote systems, while Secure File Transfer Protocol (SFTP) is an extension of SSH used specifically for securely transferring files. Both SSH and SFTP ensure that data is encrypted during transmission, protecting it from interception or tampering.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Secure Protocols and Encryption.

272. Which of the following data roles is responsible for identifying risks and appropriate access to data?

- A. Owner
- B. Custodian
- C. Steward
- D. Controller

Answer: A

Explanation:

The data owner is the role responsible for identifying risks to data and determining who should have access to that data. The owner has the authority to make decisions about the protection and usage of the data, including setting access controls and ensuring that appropriate security measures are in place.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of data governance and the roles and responsibilities associated with data management.

273. Various stakeholders are meeting to discuss their hypothetical roles and responsibilities in a specific situation, such as a security incident or major disaster.

Which of the following best describes this meeting?

- A. Penetration test
- B. Continuity of operations planning
- C. Tabletop exercise
- D. Simulation

Answer: C

Explanation:

A tabletop exercise is a discussion-based exercise where stakeholders gather to walk through the roles

and responsibilities they would have during a specific situation, such as a security incident or disaster. This type of exercise is designed to identify gaps in planning and improve coordination among team members without the need for physical execution.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of security operations and disaster recovery planning.

274. An external vendor recently visited a company's headquarters for a presentation. Following the visit a member of the hosting team found a file that the external vendor left behind on a server. The file contained detailed architecture information and code snippets.

Which of the following data types best describes this file?

- A. Government
- B. Public
- C. Proprietary
- D. Critical

Answer: C

Explanation:

The file left by the external vendor, containing detailed architecture information and code snippets, is best described as proprietary data. Proprietary data is information that is owned by a company and is essential to its competitive advantage. It includes sensitive business information such as trade secrets, intellectual property, and confidential data that should be protected from unauthorized access.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of data classification and protection.

275. The security operations center is researching an event concerning a suspicious IP address. A security analyst looks at the following event logs and discovers that a significant portion of the user accounts have experienced failed log-in attempts when authenticating from the same IP address:

```
104.168.131.241 - userA - failed authentication
104.168.131.241 - userA - failed authentication
104.168.131.241 - userB - failed authentication
104.168.131.241 - userB - failed authentication
104.168.131.241 - userC - failed authentication
104.168.131.241 - userC - failed authentication
```

Which of the following most likely describes attack that took place?

- A. Spraying
- B. Brute-force
- C. Dictionary
- D. Rainbow table

Answer: A

Explanation:

Password spraying is a type of attack where an attacker tries a small number of commonly used passwords across a large number of accounts. The event logs showing failed login attempts for many user accounts from the same IP address are indicative of a password spraying attack, where the attacker is attempting to gain access by guessing common passwords.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management and common attack vectors like password spraying.

276. Which of the following explains why an attacker cannot easily decrypt passwords using a rainbow

table attack?

- A. Digital signatures
- B. Salting
- C. Hashing
- D. Perfect forward secrecy

Answer: B

Explanation:

Salting is a technique used to enhance the security of hashed passwords by adding a unique, random value (salt) to each password before hashing it. This prevents attackers from easily decrypting passwords using rainbow tables, which are precomputed tables for reversing cryptographic hash functions. Since each password has a unique salt, the same password will produce different hash values, making rainbow table attacks ineffective.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptography and Hashing Techniques.

277. A company is currently utilizing usernames and passwords, and it wants to integrate an MFA method that is seamless, can integrate easily into a user's workflow, and can utilize employee-owned devices. Which of the following will meet these requirements?

- A. Push notifications
- B. Phone call
- C. Smart card
- D. Offline backup codes

Answer: A

Explanation:

Push notifications offer a seamless and user-friendly method of multi-factor authentication (MFA) that can easily integrate into a user's workflow. This method leverages employee-owned devices, like smartphones, to approve authentication requests through a push notification. It's convenient, quick, and doesn't require the user to input additional codes, making it a preferred choice for seamless integration with existing workflows.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

278. A financial institution would like to store its customer data in the cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The financial institution is not concerned about computational overheads and slow speeds.

Which of the following cryptographic techniques would best meet the requirement?

- A. Asymmetric
- B. Symmetric
- C. Homomorphic
- D. Ephemeral

Answer: C

Explanation:

Homomorphic encryption allows data to be encrypted and manipulated without needing to decrypt it first. This cryptographic technique would allow the financial institution to store customer data securely in the cloud while still permitting operations like searching and calculations to be performed on the encrypted data. This ensures that the cloud service provider cannot decipher the sensitive data, meeting the institution's security requirements.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptographic Techniques.

279. The Chief Information Security Officer of an organization needs to ensure recovery from ransomware would likely occur within the organization's agreed-upon RPOs and RTOs. Which of the following backup scenarios would best ensure recovery?

- A. Hourly differential backups stored on a local SAN array
- B. Daily full backups stored on premises in magnetic offline media
- C. Daily differential backups maintained by a third-party cloud provider
- D. Weekly full backups with daily incremental stored on a NAS drive

Answer: D

Explanation:

A backup strategy that combines weekly full backups with daily incremental backups stored on a NAS (Network Attached Storage) drive is likely to meet an organization's Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). This approach ensures that recent data is regularly backed up and that recovery can be done efficiently, without significant data loss or lengthy downtime.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.

CompTIA Security+ SY0-601 Study Guide: Chapter on Disaster Recovery and Backup Strategies.

280. Which of the following best describe why a process would require a two-person integrity security control?

- A. To increase the chance that the activity will be completed in half of the time the process would take only one user to complete
- B. To permit two users from another department to observe the activity that is being performed by an authorized user
- C. To reduce the risk that the procedures are performed incorrectly or by an unauthorized user
- D. To allow one person to perform the activity while being recorded on the CCTV camera

Answer: C

Explanation:

A two-person integrity security control is implemented to minimize the risk of errors or unauthorized actions. This control ensures that at least two individuals are involved in critical operations, which helps to verify the accuracy of the process and prevents unauthorized users from acting alone. It's a security measure commonly used in sensitive operations, like financial transactions or access to critical systems, to ensure accountability and accuracy.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.

CompTIA Security+ SY0-601 Study Guide: Chapter on Security Operations and Management.

281. A company recently decided to allow employees to work remotely. The company wants to protect us data without using a VPN.

Which of the following technologies should the company Implement?

- A. Secure web gateway
- B. Virtual private cloud end point
- C. Deep packet Inspection
- D. Next-gene ration firewall

Answer: A

Explanation:

A Secure Web Gateway (SWG) protects users by filtering unwanted software/malware from user-initiated web traffic and enforcing corporate and regulatory policy compliance. This technology allows the company to secure remote users' data and web traffic without relying on a VPN, making it ideal for organizations supporting remote work.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of network security and remote access technologies.

282. In a rush to meet an end-of-year business goal, the IT department was told to implement a new business application. The security engineer reviews the attributes of the application and decides the time needed to perform due diligence is insufficient from a cybersecurity perspective.

Which of the following best describes the security engineer's response?

- A. Risk tolerance
- B. Risk acceptance
- C. Risk importance
- D. Risk appetite

Answer: D

Explanation:

Risk appetite refers to the level of risk that an organization is willing to accept in order to achieve its objectives. In this scenario, the security engineer is concerned that the timeframe for implementing a new application does not allow for sufficient cybersecurity due diligence. This reflects a situation where the organization's risk appetite might be too high if it proceeds without the necessary security checks.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of risk management and understanding organizational risk appetite.

283. An organization has too many variations of a single operating system and needs to standardize the arrangement prior to pushing the system image to users.

Which of the following should the organization implement first?

- A. Standard naming convention
- B. Mashing
- C. Network diagrams
- D. Baseline configuration

Answer: D

Explanation:

Baseline configuration is the process of standardizing the configuration settings for a system or network. In this scenario, the organization needs to standardize the operating system configurations before deploying them across the network. Establishing a baseline configuration ensures that all systems adhere to the organization's security policies and operational requirements.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of system hardening and configuration management.

284. A growing company would like to enhance the ability of its security operations center to detect threats but reduce the amount of manual work required for the security analysts.

Which of the following would best enable the reduction in manual work?

- A. SOAR
- B. SIEM
- C. MDM
- D. DLP

Answer: A

Explanation:

Security Orchestration, Automation, and Response (SOAR) systems help organizations automate repetitive security tasks, reduce manual intervention, and improve the efficiency of security operations. By integrating with various security tools, SOAR can automatically respond to incidents, helping to enhance threat detection while reducing the manual workload on security analysts.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of security operations and automation technologies.

285. A systems administrator is redesigning how devices will perform network authentication.

The following requirements need to be met:

- An existing Internal certificate must be used.
- Wired and wireless networks must be supported
- Any unapproved device should be Isolated in a quarantine subnet
- Approved devices should be updated before accessing resources

Which of the following would best meet the requirements?

- A. 802.1X
- B. EAP
- C. RADIUS
- D. WPA2

Answer: A

Explanation:

802.1X is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. It supports the use of certificates for authentication, can quarantine unapproved devices, and ensures that only approved and updated devices can access network resources. This protocol best meets the requirements of securing both wired and wireless networks with internal certificates.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of network security and authentication protocols.

286. A company implemented an MDM policy to mitigate risks after repeated instances of employees losing company-provided mobile phones. In several cases, the lost phones were used maliciously to perform social engineering attacks against other employees.

Which of the following MDM features should be configured to best address this issue? (Select two).

- A. Screen locks
- B. Remote wipe
- C. Full device encryption
- D. Push notifications
- E. Application management
- F. Geolocation

Answer: B, A

Explanation:

Integrating each SaaS solution with an Identity Provider (IdP) is the most effective way to address the security issue. This approach allows for Single Sign-On (SSO) capabilities, where users can access multiple SaaS applications with a single set of credentials while maintaining strong password policies across all services. It simplifies the user experience and ensures consistent security enforcement across different SaaS platforms.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

287. A security analyst needs to propose a remediation plan for each item in a risk register. The item with the highest priority requires employees to have separate logins for SaaS solutions and different password complexity requirements for each solution.

Which of the following implementation plans will most likely resolve this security issue?

- A. Creating a unified password complexity standard
- B. Integrating each SaaS solution with the Identity provider
- C. Securing access to each SaaS by using a single wildcard certificate
- D. Configuring geofencing on each SaaS solution

Answer: B

Explanation:

Integrating each SaaS solution with an Identity Provider (IdP) is the most effective way to address the security issue. This approach allows for Single Sign-On (SSO) capabilities, where users can access multiple SaaS applications with a single set of credentials while maintaining strong password policies across all services. It simplifies the user experience and ensures consistent security enforcement across different SaaS platforms.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

288. A security analyst finds a rogue device during a monthly audit of current endpoint assets that are connected to the network. The corporate network utilizes 802.1X for access control. To be allowed on the network, a device must have a Known hardware address, and a valid user name and password must be entered in a captive portal.

The following is the audit report:

IP address	MAC	Host	Account
10.10.04.42	EE-AC-11-F3-E4-44	PC-NY	user1
10.10.04.38	EE-AC-11-82-42-F3	PC-CA	user3
10.10.04.59	28-BB-5A-11-52-29	PC-PA	user2
10.10.04.50	28-BB-5A-F0-E9-D1	PC-TX	user4
10.10.04.22	EE-AC-11-82-42-F3	WIN10	user3
10.10.04.26	EE-28-11-21-A2-73	PC-NJ	admin

Which of the following is the most likely way a rogue device was allowed to connect?

- A. A user performed a MAC cloning attack with a personal device.
- B. A DMCP failure caused an incorrect IP address to be distributed
- C. An administrator bypassed the security controls for testing.
- D. DNS hijacking let an attacker intercept the captive portal traffic.

Answer: A

Explanation:

The most likely way a rogue device was able to connect to the network is through a MAC cloning attack. In this attack, a personal device copies the MAC address of an authorized device, bypassing the 802.1X access control that relies on known hardware addresses for network access. The matching MAC addresses in the audit report suggest that this technique was used to gain unauthorized network access.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Network Security and MAC Address Spoofing.

289. Which of the following is the first step to take when creating an anomaly detection process?

- A. Selecting events
- B. Building a baseline
- C. Selecting logging options
- D. Creating an event log

Answer: B

Explanation:

The first step in creating an anomaly detection process is building a baseline of normal behavior within the system. This baseline serves as a reference point to identify deviations or anomalies that could indicate a security incident. By understanding what normal activity looks like, security teams can more effectively detect and respond to suspicious behavior.

Reference =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Monitoring and Baselines.

290. Which of the following is the final step of the modern response process?

- A. Lessons learned
- B. Eradication
- C. Containment
- D. Recovery

Answer: A

Explanation:

The final step in the incident response process is "Lessons learned." This step involves reviewing and

analyzing the incident to understand what happened, how it was handled, and what could be improved. The goal is to improve future response efforts and prevent similar incidents from occurring. It's essential for refining the incident response plan and enhancing overall security posture.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of incident response and recovery.

291. While investigating a recent security breach an analyst finds that an attacker gained access by SQL injection through a company website.

Which of the following should the analyst recommend to the website developers to prevent this from reoccurring?

- A. Secure cookies
- B. Input sanitization
- C. Code signing
- D. Blocklist

Answer: B

Explanation:

Input sanitization is a critical security measure to prevent SQL injection attacks, which occur when an attacker exploits vulnerabilities in a website's input fields to execute malicious SQL code. By properly sanitizing and validating all user inputs, developers can prevent malicious code from being executed, thereby securing the website against such attacks.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of web application security and common vulnerability mitigation strategies.

292. Which of the following environments utilizes a subset of customer data and is most likely to be used to assess the impacts of major system upgrades and demonstrate system features?

- A. Development
- B. Test
- C. Production
- D. Staging

Answer: D

Explanation:

A staging environment is a controlled setting that closely mirrors the production environment but uses a subset of customer data. It is used to test major system upgrades, assess their impact, and demonstrate new features before they are rolled out to the live production environment. This ensures that any issues can be identified and addressed in a safe environment before affecting end-users.

Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of secure system development and testing environments.

293. An organization recently started hosting a new service that customers access through a web portal. A security engineer needs to add to the existing security devices a new solution to protect this new service.

Which of the following is the engineer most likely to deploy?

- A. Layer 4 firewall
- B. NGFW

C. WAF

D. UTM

Answer: C

Explanation:

The security engineer is likely to deploy a Web Application Firewall (WAF) to protect the new web portal service. A WAF specifically protects web applications by filtering, monitoring, and blocking HTTP requests based on a set of rules. This is crucial for preventing common attacks such as SQL injection, cross-site scripting (XSS), and other web-based attacks that could compromise the web service.

Layer 4 firewall operates primarily at the transport layer, focusing on IP address and port filtering, making it unsuitable for web application-specific threats.

NGFW (Next-Generation Firewall) provides more advanced filtering than traditional firewalls, including layer 7 inspection, but the WAF is tailored specifically for web traffic.

UTM (Unified Threat Management) offers a suite of security tools in one package (like antivirus, firewall, and content filtering), but for web application-specific protection, a WAF is the best fit.

294. An IT manager is putting together a documented plan describing how the organization will keep operating in the event of a global incident.

Which of the following plans is the IT manager creating?

A. Business continuity

B. Physical security

C. Change management

D. Disaster recovery

Answer: A

Explanation:

The IT manager is creating a Business Continuity Plan (BCP). A BCP describes how an organization will continue to operate during and after a disaster or global incident. It ensures that critical business functions remain operational despite adverse conditions, with a focus on minimizing downtime and maintaining essential services.

Physical security relates to protecting physical assets.

Change management ensures changes in IT systems are introduced smoothly, without disrupting operations.

Disaster recovery is a subset of business continuity but focuses specifically on recovering from IT-related incidents.

295. Which of the following topics would most likely be included within an organization's SDLC?

A. Service-level agreements

B. Information security policy

C. Penetration testing methodology

D. Branch protection requirements

Answer: B

Explanation:

Within an organization's Software Development Life Cycle (SDLC), an Information Security Policy is a vital component. It outlines the rules and procedures for ensuring that the organization's IT assets and data are protected throughout the development process. Ensuring secure coding practices, access

controls, and regular security testing is fundamental in preventing vulnerabilities in applications. Other options like service-level agreements and branch protection requirements are less likely to be integral to SDLC processes. Penetration testing methodology, while useful, is generally considered outside the scope of the SDLC.

296. Which of the following describes the understanding between a company and a client about what will be provided and the accepted time needed to provide the company with the resources?

- A. SLA
- B. MOU
- C. MOA
- D. BPA

Answer: A

Explanation:

A Service Level Agreement (SLA) is a formal document between a service provider and a client that defines the expected level of service, including what resources will be provided and the agreed-upon time frames. It typically includes metrics to evaluate performance, uptime guarantees, and response times.

MOU (Memorandum of Understanding) and MOA (Memorandum of Agreement) are less formal and may not specify the exact level of service.

BPA (Business Partners Agreement) focuses more on the long-term relationship between partners.

297. Which of the following describes an executive team that is meeting in a board room and testing the company's incident response plan?

- A. Continuity of operations
- B. Capacity planning
- C. Tabletop exercise
- D. Parallel processing

Answer: C

Explanation:

A tabletop exercise involves the executive team or key stakeholders discussing and testing the company's incident response plan in a simulated environment. These exercises are low-stress, discussion-based, and help to validate the plan's effectiveness by walking through different scenarios without disrupting actual operations. It is an essential part of testing business continuity and incident response strategies.

Continuity of operations refers to the ability of an organization to continue functioning during and after a disaster but doesn't specifically involve simulations like tabletop exercises.

Capacity planning is related to ensuring the infrastructure can handle growth, not incident response testing.

Parallel processing refers to running multiple processes simultaneously, which is unrelated to testing an incident response plan.

298. Which of the following methods would most likely be used to identify legacy systems?

- A. Bug bounty program
- B. Vulnerability scan

C. Package monitoring

D. Dynamic analysis

Answer: B

Explanation:

A vulnerability scan is the most likely method to identify legacy systems. These scans assess an organization's network and systems for known vulnerabilities, including outdated or unsupported software (i.e., legacy systems) that may pose a security risk. The scan results can highlight systems that are no longer receiving updates, helping IT teams address these risks.

Bug bounty programs are used to incentivize external researchers to find security flaws, but they are less effective at identifying legacy systems.

Package monitoring tracks installed software packages for updates or issues but is not as comprehensive for identifying legacy systems.

Dynamic analysis is typically used for testing applications during runtime to find vulnerabilities, but not for identifying legacy systems.

299. Which of the following considerations is the most important for an organization to evaluate as it establishes and maintains a data privacy program?

A. Reporting structure for the data privacy officer

B. Request process for data subject access

C. Role as controller or processor

D. Physical location of the company

Answer: C

Explanation:

The most important consideration when establishing a data privacy program is defining the organization's role as a controller or processor. These roles, as outlined in privacy regulations such as the General Data Protection Regulation (GDPR), determine the responsibilities regarding the handling of personal data. A controller is responsible for determining the purpose and means of data processing, while a processor acts on behalf of the controller. This distinction is crucial for compliance with data privacy laws.

Reporting structure for the data privacy officer is important, but it is a secondary consideration compared to legal roles.

Request process for data subject access is essential for compliance but still depends on the organization's role as controller or processor.

Physical location of the company can affect jurisdiction, but the role as controller or processor has a broader and more immediate impact.

300. Client files can only be accessed by employees who need to know the information and have specified roles in the company.

Which of the following best describes this security concept?

A. Availability

B. Confidentiality

C. Integrity

D. Non-repudiation

Answer: B

Explanation:

The scenario described, where client files are only accessible to employees who "need to know" the information, reflects the concept of confidentiality. Confidentiality ensures that sensitive information is only accessible to those who are authorized to view it, preventing unauthorized access.

Availability ensures that data is accessible when needed but doesn't focus on restricting access.

Integrity ensures that data remains accurate and unaltered but doesn't pertain to access control.

Non-repudiation ensures that actions cannot be denied after they are performed, but this concept is unrelated to access control.

301. A user would like to install software and features that are not available with a smartphone's default software.

Which of the following would allow the user to install unauthorized software and enable new features?

- A. SOU
- B. Cross-site scripting
- C. Jailbreaking
- D. Side loading

Answer: C

Explanation:

Jailbreaking is the process of removing restrictions imposed by the manufacturer on a smartphone, allowing the user to install unauthorized software and features not available through official app stores. This action typically voids the warranty and can introduce security risks by bypassing built-in protections.

SOU (Statement of Understanding) is not related to modifying devices.

Cross-site scripting is a web-based attack technique, unrelated to smartphone software.

Side loading refers to installing apps from unofficial sources but without necessarily removing built-in restrictions like jailbreaking does.

302. A recent penetration test identified that an attacker could flood the MAC address table of network switches.

Which of the following would best mitigate this type of attack?

- A. Load balancer
- B. Port security
- C. IPS
- D. NGFW

Answer: B

Explanation:

Port security is the best mitigation technique for preventing an attacker from flooding the MAC address table of network switches. Port security can limit the number of MAC addresses learned on a port, preventing an attacker from overwhelming the switch's MAC table (a form of MAC flooding attack). When the allowed number of MAC addresses is exceeded, port security can block additional devices or trigger alerts.

Load balancer distributes network traffic but does not address MAC flooding attacks.

IPS (Intrusion Prevention System) detects and prevents attacks but isn't specifically designed for MAC flooding mitigation.

NGFW (Next-Generation Firewall) offers advanced traffic inspection but is not directly involved in MAC

table security.

303. An administrator at a small business notices an increase in support calls from employees who receive a blocked page message after trying to navigate to a spoofed website.

Which of the following should the administrator do?

- A. Deploy multifactor authentication.
- B. Decrease the level of the web filter settings
- C. Implement security awareness training.
- D. Update the acceptable use policy

Answer: C

Explanation:

In this scenario, employees are attempting to navigate to spoofed websites, which is being blocked by the web filter. To address this issue, the administrator should implement security awareness training. Training helps employees recognize phishing and other social engineering attacks, reducing the likelihood that they will attempt to access malicious websites in the future.

Deploying multifactor authentication (MFA) would strengthen authentication but does not directly address user behavior related to phishing websites.

Decreasing the level of the web filter would expose the organization to more threats.

Updating the acceptable use policy may clarify guidelines but is not as effective as hands-on training for improving user behavior.

304. Which of the following control types is AUP an example of?

- A. Physical
- B. Managerial
- C. Technical
- D. Operational

Answer: B

Explanation:

An Acceptable Use Policy (AUP) is an example of a managerial control. Managerial controls are policies and procedures that govern an organization's operations, ensuring security through directives and rules. The AUP defines acceptable behavior and usage of company resources, setting guidelines for employees.

Physical controls refer to security measures like locks, fences, or security guards.

Technical controls involve security mechanisms such as firewalls or encryption.

Operational controls are procedures for maintaining security, such as backup and recovery plans.

305. Which of the following examples would be best mitigated by input sanitization?

- A. `<script>alert ("Warning!") ,-</script>`
- B. `nmap - 10.11.1.130`
- C. Email message: "Click this link to get your free gift card."
- D. Browser message: "Your connection is not private."

Answer: A

Explanation:

This example of a script injection attack would be best mitigated by input sanitization. Input sanitization

involves cleaning or filtering user inputs to ensure that they do not contain harmful data, such as malicious scripts. This prevents attackers from executing script-based attacks (e.g., Cross-Site Scripting or XSS).

Nmap command is unrelated to input sanitization, as it is a network scanning tool.

Email phishing attempts require different mitigations, such as user training.

Browser warnings about insecure connections involve encryption protocols, not input validation

306. A security engineer is installing an IPS to block signature-based attacks in the environment. Which of the following modes will best accomplish this task?

- A. Monitor
- B. Sensor
- C. Audit
- D. Active

Answer: D

Explanation:

To block signature-based attacks, the Intrusion Prevention System (IPS) must be in active mode. In this mode, the IPS can actively monitor and block malicious traffic in real time based on predefined signatures. This is the best mode to prevent known attack types from reaching the internal network. Monitor mode and sensor mode are typically passive, meaning they only observe and log traffic without actively blocking it.

Audit mode is used for review purposes and does not actively block traffic.

307. An organization wants to limit potential impact to its log-in database in the event of a breach. Which of the following options is the security team most likely to recommend?

- A. Tokenization
- B. Hashing
- C. Obfuscation
- D. Segmentation

Answer: B

Explanation:

To limit the potential impact on the log-in database in case of a breach, the security team would most likely recommend hashing. Hashing converts passwords into fixed-length strings of characters, which cannot be easily reversed to reveal the original passwords. Even if the database is breached, attackers cannot easily retrieve the actual passwords if they are properly hashed (especially with techniques like salting).

Tokenization is used to replace sensitive data with a token, but it is more common for protecting credit card data than passwords.

Obfuscation is the process of making data harder to interpret but is weaker than hashing for password protection.

Segmentation helps isolate data but doesn't directly protect the contents of the login database.

308. A visitor plugs a laptop into a network jack in the lobby and is able to connect to the company's network.

Which of the following should be configured on the existing network infrastructure to best prevent this

activity?

- A. Port security
- B. Web application firewall
- C. Transport layer security
- D. Virtual private network

Answer: A

Explanation:

Port security is the best solution to prevent unauthorized devices, like a visitor's laptop, from connecting to the company's network. Port security can limit the number of devices that can connect to a network switch port and block unauthorized MAC addresses, effectively stopping unauthorized access attempts. Web application firewall (WAF) protects against web-based attacks, not unauthorized network access. Transport Layer Security (TLS) ensures encrypted communication but does not manage physical network access.

Virtual Private Network (VPN) secures remote connections but does not control access through physical network ports.

309. During a penetration test, a vendor attempts to enter an unauthorized area using an access badge. Which of the following types of tests does this represent?

- A. Defensive
- B. Passive
- C. Offensive
- D. Physical

Answer: D

Explanation:

Attempting to enter an unauthorized area using an access badge during a penetration test is an example of a physical test. This type of test evaluates the effectiveness of physical security controls, such as access badges, security guards, and locks, in preventing unauthorized access to restricted areas. Defensive and offensive testing typically refer to digital or network-based penetration testing strategies. Passive testing involves observing or monitoring but not interacting with the environment.

310. An organization experiences a cybersecurity incident involving a command-and-control server. Which of the following logs should be analyzed to identify the impacted host? (Select two).

- A. Application
- B. Authentication
- C. DHCP
- D. Network
- E. Firewall
- F. Database

Answer: C, E

Explanation:

To identify the impacted host in a command-and-control (C2) server incident, the following logs should be analyzed:

DHCP logs: These logs record IP address assignments. By reviewing DHCP logs, an organization can determine which host was assigned a specific IP address during the time of the attack.

Firewall logs: Firewall logs will show traffic patterns, including connections to external C2 servers. Analyzing these logs helps to identify the IP address and port numbers of the communicating host. Application, Authentication, and Database logs are less relevant in this context because they focus on internal processes and authentication events rather than network traffic involved in a C2 attack.

311. Which of the following should a security operations center use to improve its incident response procedure?

- A. Playbooks
- B. Frameworks
- C. Baselines
- D. Benchmarks

Answer: A

Explanation:

A playbook is a documented set of procedures that outlines the step-by-step response to specific types of cybersecurity incidents. Security Operations Centers (SOCs) use playbooks to improve consistency, efficiency, and accuracy during incident response. Playbooks help ensure that the correct procedures are followed based on the type of incident, ensuring swift and effective remediation.

Frameworks provide general guidelines for implementing security but are not specific enough for incident response procedures.

Baselines represent normal system behavior and are used for anomaly detection, not incident response guidance.

Benchmarks are performance standards and are not directly related to incident response.

312. An administrator has identified and fingerprinted specific files that will generate an alert if an attempt is made to email these files outside of the organization.

Which of the following best describes the tool the administrator is using?

- A. DLP
- B. SNMP traps
- C. SCAP
- D. IPS

Answer: A

Explanation:

The administrator is using a Data Loss Prevention (DLP) tool, which is designed to identify, monitor, and protect sensitive data. By fingerprinting specific files, DLP ensures that these files cannot be emailed or sent outside the organization without triggering an alert or blocking the action. This is a key feature of DLP systems, which prevent data exfiltration and ensure data security compliance.

SNMP traps are used for network management and monitoring, not data protection.

SCAP (Security Content Automation Protocol) is a set of standards for automating vulnerability management and policy compliance, unrelated to file monitoring.

IPS (Intrusion Prevention System) blocks network-based attacks but does not handle file fingerprinting.

313. A security analyst is investigating a workstation that is suspected of outbound communication to a command-and-control server. During the investigation, the analyst discovered that logs on the endpoint were deleted.

Which of the following logs would the analyst most likely look at next?

- A. IPS
- B. Firewall
- C. ACL
- D. Windows security

Answer: B

Explanation:

Since the logs on the endpoint were deleted, the next best option for the analyst is to examine firewall logs. Firewall logs can reveal external communication, including outbound traffic to a command-and-control (C2) server. These logs would contain information about the IP addresses, ports, and protocols used, which can help in identifying suspicious connections.

IPS logs may provide information about network intrusions, but firewall logs are better for tracking communication patterns.

ACL logs (Access Control List) are useful for tracking access permissions but not for identifying C2 communication.

Windows security logs would have been ideal if they had not been deleted

314. A security team is setting up a new environment for hosting the organization's on-premises software application as a cloud-based service.

Which of the following should the team ensure is in place in order for the organization to follow security best practices?

- A. Visualization and isolation of resources
- B. Network segmentation
- C. Data encryption
- D. Strong authentication policies

Answer: A

Explanation:

When hosting an on-premises software application in a cloud-based service, ensuring visualization and isolation of resources is crucial for maintaining security best practices. This involves using virtualization techniques to create isolated environments (e.g., virtual machines or containers) for different applications and services, reducing the risk of cross-tenant attacks or resource leakage.

Network segmentation is important but pertains more to securing network traffic rather than isolating computing resources.

Data encryption is also essential but doesn't specifically address resource isolation in a cloud environment.

Strong authentication policies are critical for access control but do not address the need for isolating resources within the cloud environment.

315. Which of the following phases of an incident response involves generating reports?

- A. Recovery
- B. Preparation
- C. Lessons learned
- D. Containment

Answer: C

Explanation:

The lessons learned phase of an incident response process involves reviewing the incident and generating reports. This phase helps identify what went well, what needs improvement, and what changes should be made to prevent future incidents. Documentation and reporting are essential parts of this phase to ensure that the findings are recorded and used for future planning.

Recovery focuses on restoring services and normal operations.

Preparation involves creating plans and policies for potential incidents, not reporting.

Containment deals with isolating and mitigating the effects of the incident, not generating reports.

316. A business needs a recovery site but does not require immediate failover. The business also wants to reduce the workload required to recover from an outage.

Which of the following recovery sites is the best option?

- A. Hot
- B. Cold
- C. Warm
- D. Geographically dispersed

Answer: C

Explanation:

A warm site is the best option for a business that does not require immediate failover but wants to reduce the workload required for recovery. A warm site has some pre-installed equipment and data, allowing for quicker recovery than a cold site, but it still requires some setup before becoming fully operational.

Hot sites provide immediate failover but are more expensive and require constant maintenance.

Cold sites require significant time and effort to get up and running after an outage.

Geographically dispersed sites refer to a specific location strategy rather than the readiness of the recovery site.

317. Which of the following best describes the practice of researching laws and regulations related to information security operations within a specific industry?

- A. Compliance reporting
- B. GDPR
- C. Due diligence
- D. Attestation

Answer: C

Explanation:

Due diligence refers to the process of researching and understanding the laws, regulations, and best practices that govern information security within a specific industry. Organizations are required to conduct due diligence to ensure compliance with legal and regulatory requirements, which helps mitigate risks and avoid penalties.

Compliance reporting involves generating reports to demonstrate adherence to legal or regulatory standards.

GDPR is a specific regulation governing data privacy in the EU, not a general practice of researching laws.

Attestation is a formal declaration that an organization is compliant with a set of standards but is not the act of researching the laws.

318. A security analyst developed a script to automate a trivial and repeatable task.

Which of the following best describes the benefits of ensuring other team members understand how the script works?

- A. To reduce implementation cost
- B. To identify complexity
- C. To remediate technical debt
- D. To prevent a single point of failure

Answer: D

Explanation:

Ensuring that other team members understand how a script works is essential to prevent a single point of failure. If only one person knows how the script operates, the organization risks being unable to maintain or troubleshoot it if that person is unavailable. Sharing knowledge ensures continuity and reduces dependence on one individual.

Reducing implementation cost and remediating technical debt are secondary considerations in this context.

Identifying complexity is important, but the main benefit is to avoid a single point of failure.

319. A bank set up a new server that contains customers' PII.

Which of the following should the bank use to make sure the sensitive data is not modified?

- A. Full disk encryption
- B. Network access control
- C. File integrity monitoring
- D. User behavior analytics

Answer: C

Explanation:

To ensure that sensitive data, such as Personally Identifiable Information (PII), is not modified, the bank should implement file integrity monitoring (FIM). FIM tracks changes to files and provides alerts if unauthorized modifications are detected, ensuring data integrity.

Full disk encryption protects data at rest but does not prevent or monitor modifications.

Network access control (NAC) manages access to the network but doesn't monitor file changes.

User behavior analytics (UBA) detects suspicious user activities but is not focused on file integrity.

320. A legacy device is being decommissioned and is no longer receiving updates or patches.

Which of the following describes this scenario?

- A. End of business
- B. End of testing
- C. End of support
- D. End of life

Answer: D

Explanation:

When a legacy device is no longer receiving updates or patches, it is considered to be at the end of life (EOL). This means the manufacturer has ceased support for the device, and it will no longer receive updates, security patches, or technical assistance. EOL devices pose security risks and are often

decommissioned or replaced.

End of support may seem similar but typically refers to the cessation of technical support, whereas EOL means the device is fully retired.

End of business and End of testing do not apply in this context.

321. Employees located off-site must have access to company resources in order to complete their assigned tasks. These employees utilize a solution that allows remote access without interception concerns.

Which of the following best describes this solution?

- A. Proxy server
- B. NGFW
- C. VPN
- D. Security zone

Answer: C

Explanation:

A Virtual Private Network (VPN) is the best solution to allow remote employees secure access to company resources without interception concerns. A VPN establishes an encrypted tunnel over the internet, ensuring that data transferred between remote employees and the company is secure from eavesdropping.

Proxy server helps with web content filtering and anonymization but does not provide encrypted access. NGFW (Next-Generation Firewall) enhances security but is not the primary tool for enabling remote access.

Security zone is a network segmentation technique but does not provide remote access capabilities.

322. Which of the following alert types is the most likely to be ignored over time?

- A. True positive
- B. True negative
- C. False positive
- D. False negative

Answer: C

Explanation:

A false positive is an alert that incorrectly identifies benign activity as malicious. Over time, if an alerting system generates too many false positives, security teams are likely to ignore these alerts, resulting in "alert fatigue." This increases the risk of missing genuine threats.

True positives and true negatives are accurate and should be acted upon.

False negatives are more dangerous because they fail to identify real threats, but they are not "ignored" since they do not trigger alerts.

323. The Chief Information Security Officer (CISO) at a large company would like to gain an understanding of how the company's security policies compare to the requirements imposed by external regulators.

Which of the following should the CISO use?

- A. Penetration test
- B. Internal audit

- C. Attestation
- D. External examination

Answer: D

Explanation:

An external examination (also known as an external audit or external review) is the best method for the Chief Information Security Officer (CISO) to gain an understanding of how the company's security policies compare to external regulatory requirements. External examinations are conducted by third-party entities that assess an organization's compliance with laws, regulations, and industry standards. Penetration tests focus on identifying vulnerabilities, not compliance. Internal audits assess internal controls but are not impartial or focused on regulatory requirements. Attestation is a formal declaration but does not involve the actual evaluation of compliance.

324. A systems administrator notices that one of the systems critical for processing customer transactions is running an end-of-life operating system.

Which of the following techniques would increase enterprise security?

- A. Installing HIDS on the system
- B. Placing the system in an isolated VLAN
- C. Decommissioning the system
- D. Encrypting the system's hard drive

Answer: B

Explanation:

To enhance security for a system running an end-of-life operating system, placing the system in an isolated VLAN is the most effective approach. By isolating the system from the rest of the network, you can limit its exposure to potential threats while maintaining its functionality. This segmentation helps protect the rest of the network from any vulnerabilities in the outdated system.

Installing HIDS (Host-based Intrusion Detection System) can help detect intrusions but won't mitigate the risks posed by an unsupported OS.

Decommissioning may not be feasible if the system is critical.

Encrypting the system's hard drive protects data at rest but doesn't address vulnerabilities from an outdated OS.

325. An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use. Each application has a separate log-in. so the security team wants to reduce the number of credentials each employee must maintain.

Which of the following is the first step the security team should take?

- A. Enable SAML
- B. Create OAuth tokens.
- C. Use password vaulting.
- D. Select an IdP

Answer: D

Explanation:

The first step in reducing the number of credentials each employee must maintain when using multiple SaaS applications is to select an Identity Provider (IdP). An IdP provides a centralized authentication service that supports Single Sign-On (SSO), enabling users to access multiple applications with a single

set of credentials.

Enabling SAML would be part of the technical implementation but comes after selecting an IdP.

OAuth tokens are used for authorization, but selecting an IdP is the first step in managing authentication.

Password vaulting stores multiple passwords securely but doesn't reduce the need for separate logins.

326. Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?

- A. To track the status of patching installations
- B. To find shadow IT cloud deployments
- C. To continuously the monitor hardware inventory
- D. To hunt for active attackers in the network

Answer: A

Explanation:

Running daily vulnerability scans on all corporate endpoints is primarily done to track the status of patching installations. These scans help identify any missing security patches or vulnerabilities that could be exploited by attackers. Keeping the endpoints up-to-date with the latest patches is critical for maintaining security.

Finding shadow IT cloud deployments and monitoring hardware inventory are better achieved through other tools.

Hunting for active attackers would typically involve more real-time threat detection methods than daily vulnerability scans.

327. Which of the following threat vectors is most commonly utilized by insider threat actors attempting data exfiltration?

- A. Unidentified removable devices
- B. Default network device credentials
- C. Spear phishing emails
- D. Impersonation of business units through typo squatting

Answer: A

Explanation:

Unidentified removable devices, such as USB drives, are a common threat vector for insider threat actors attempting data exfiltration. Insiders can easily use these devices to transfer sensitive data out of the organization undetected, making it one of the most commonly utilized methods for data theft.

Default network device credentials are a security vulnerability but not typically used for data exfiltration.

Spear phishing emails are used for external attacks, not insider data exfiltration.

Impersonation through typo squatting is typically used by external actors for phishing or fraud.

328. A new employee logs in to the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company.

Which of the following attack vectors is most likely being used?

- A. Business email
- B. Social engineering
- C. Unsecured network

D. Default credentials

Answer: B

Explanation:

The employee notices that the links in the email do not correspond to the company's official URLs, indicating that this is likely a social engineering attack. Social engineering involves manipulating individuals into divulging confidential information or performing actions that may compromise security. Phishing emails, like the one described, often contain fraudulent links to trick the recipient into providing sensitive information or downloading malware.

Business email refers to business email compromise (BEC), which typically involves impersonating a high-level executive to defraud the company.

Unsecured network is unrelated to the email content.

Default credentials do not apply here, as the issue is with suspicious links, not login credentials.

329. An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment.

Which of the following solutions would mitigate the risk?

A. XDR

B. SPF

C. DLP

D. DMARC

Answer: C

Explanation:

To mitigate the risk of sensitive data being exfiltrated from the environment, the IT manager should implement a Data Loss Prevention (DLP) solution. DLP monitors and controls the movement of sensitive data, ensuring that unauthorized transfers are blocked and potential data breaches are prevented.

XDR (Extended Detection and Response) is useful for threat detection across multiple environments but doesn't specifically address data exfiltration.

SPF (Sender Policy Framework) helps prevent email spoofing, not data exfiltration.

DMARC (Domain-based Message Authentication, Reporting & Conformance) also addresses email security and spoofing, not data exfiltration.

330. An important patch for a critical application has just been released, and a systems administrator is identifying all of the systems requiring the patch.

Which of the following must be maintained in order to ensure that all systems requiring the patch are updated?

A. Asset inventory

B. Network enumeration

C. Data certification

D. Procurement process

Answer: A

Explanation:

To ensure that all systems requiring the patch are updated, the systems administrator must maintain an accurate asset inventory. This inventory lists all hardware and software assets within the organization, allowing the administrator to identify which systems are affected by the patch and ensuring that none are

missed during the update process.

Network enumeration is used to discover devices on a network but doesn't track software that requires patching.

Data certification and procurement process are unrelated to tracking systems for patching purposes.

331. A company is decommissioning its physical servers and replacing them with an architecture that will reduce the number of individual operating systems.

Which of the following strategies should the company use to achieve this security requirement?

- A. Microservices
- B. Containerization
- C. Virtualization
- D. Infrastructure as code

Answer: B

Explanation:

To reduce the number of individual operating systems while decommissioning physical servers, the company should use containerization. Containerization allows multiple applications to run in isolated environments on a single operating system, significantly reducing the overhead compared to running multiple virtual machines, each with its own OS.

Containerization: Uses containers to run multiple isolated applications on a single OS kernel, reducing the need for multiple OS instances and improving resource utilization.

Microservices: An architectural style that structures an application as a collection of loosely coupled services, which does not necessarily reduce the number of operating systems.

Virtualization: Allows multiple virtual machines to run on a single physical server, but each VM requires its own OS, not reducing the number of OS instances.

Infrastructure as code: Manages and provisions computing infrastructure through machine-readable configuration files, but it does not directly impact the number of operating systems.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 3.1 - Compare and contrast security implications of different architecture models (Containerization).

332. An organization wants to ensure the integrity of compiled binaries in the production environment.

Which of the following security measures would best support this objective?

- A. Input validation
- B. Code signing
- C. SQL injection
- D. Static analysis

Answer: B

Explanation:

To ensure the integrity of compiled binaries in the production environment, the best security measure is code signing. Code signing uses digital signatures to verify the authenticity and integrity of the software, ensuring that the code has not been tampered with or altered after it was signed. Code signing: Involves signing code with a digital signature to verify its authenticity and integrity, ensuring the compiled binaries have not been altered.

Input validation: Ensures that only properly formatted data enters an application but does not verify the integrity of compiled binaries.

SQL injection: A type of attack, not a security measure.

Static analysis: Analyzes code for vulnerabilities and errors but does not ensure the integrity of compiled binaries in production.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.4 - Explain the importance of using appropriate cryptographic solutions (Code signing).

333. A systems administrator would like to deploy a change to a production system.

Which of the following must the administrator submit to demonstrate that the system can be restored to a working state in the event of a performance issue?

- A. Backout plan
- B. Impact analysis
- C. Test procedure
- D. Approval procedure

Answer: A

Explanation:

To demonstrate that the system can be restored to a working state in the event of a performance issue after deploying a change, the systems administrator must submit a backout plan. A backout plan outlines the steps to revert the system to its previous state if the new deployment causes problems.

Backout plan: Provides detailed steps to revert changes and restore the system to its previous state in case of issues, ensuring minimal disruption and quick recovery.

Impact analysis: Evaluates the potential effects of a change but does not provide steps to revert changes.

Test procedure: Details the steps for testing the change but does not address restoring the system to a previous state.

Approval procedure: Involves obtaining permissions for the change but does not ensure system recovery in case of issues.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.3 - Explain the importance of change management processes (Backout plan).

334. A security administrator is configuring fileshares. The administrator removed the default permissions and added permissions for only users who will need to access the fileshares as part of their job duties.

Which of the following best describes why the administrator performed these actions?

- A. Encryption standard compliance
- B. Data replication requirements
- C. Least privilege
- D. Access control monitoring

Answer: C

Explanation:

The security administrator's actions of removing default permissions and adding permissions only for users who need access as part of their job duties best describe the principle of least privilege. This principle ensures that users are granted the minimum necessary access to perform their job functions, reducing the risk of unauthorized access or data breaches.

Least privilege: Limits access rights for users to the bare minimum necessary for their job duties, enhancing security by reducing potential attack surfaces.

Encryption standard compliance: Involves meeting encryption requirements, but it does not explain the removal and assignment of specific permissions.

Data replication requirements: Focus on duplicating data across different systems for redundancy and availability, not related to user permissions.

Access control monitoring: Involves tracking and reviewing access to resources, but the scenario is about setting permissions, not monitoring them.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.5 - Modify enterprise capabilities to enhance security (Least privilege).

335. Which of the following describes effective change management procedures?

- A. Approving the change after a successful deployment
- B. Having a backout plan when a patch fails
- C. Using a spreadsheet for tracking changes
- D. Using an automatic change control bypass for security updates

Answer: B

Explanation:

Effective change management procedures include having a backout plan when a patch fails. A backout plan ensures that there are predefined steps to revert the system to its previous state if the new change or patch causes issues, thereby minimizing downtime and mitigating potential negative impacts.

Having a backout plan when a patch fails: Essential for ensuring that changes can be safely reverted in case of problems, maintaining system stability and availability.

Approving the change after a successful deployment: Changes should be approved before deployment, not after.

Using a spreadsheet for tracking changes: While useful for documentation, it is not a comprehensive change management procedure.

Using an automatic change control bypass for security updates: Bypassing change control can lead to unapproved and potentially disruptive changes.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.3 - Explain the importance of change management processes (Backout plan).

336. Which of the following tasks is typically included in the BIA process?

- A. Estimating the recovery time of systems
- B. Identifying the communication strategy
- C. Evaluating the risk management plan
- D. Establishing the backup and recovery procedures
- E. Developing the incident response plan

Answer: A

Explanation:

Estimating the recovery time of systems is a task typically included in the Business Impact Analysis (BIA) process. BIA involves identifying the critical functions of a business and determining the impact of a disruption. This includes estimating how long it will take to recover systems and resume normal operations.

Estimating the recovery time of systems: A key component of BIA, which helps in understanding the time needed to restore systems and services after a disruption.

Identifying the communication strategy: Typically part of the incident response plan, not BIA.

Evaluating the risk management plan: Part of risk management, not specifically BIA.

Establishing the backup and recovery procedures: Important for disaster recovery, not directly part of BIA.

Developing the incident response plan: Focuses on responding to security incidents, not on the impact analysis.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 5.2 - Risk management process (Business Impact Analysis - BIA).

337. An administrator needs to perform server hardening before deployment.

Which of the following steps should the administrator take? (Select two).

- A. Disable default accounts.
- B. Add the server to the asset inventory.
- C. Remove unnecessary services.
- D. Document default passwords.
- E. Send server logs to the SIEM.
- E. Join the server to the corporate domain.

Answer: A, C

Explanation:

To perform server hardening before deployment, the administrator should disable default accounts and remove unnecessary services. These steps are crucial to reducing the attack surface and enhancing the security of the server.

Disable default accounts: Default accounts often come with default credentials that are well-known and can be exploited by attackers. Disabling these accounts helps prevent unauthorized access. Remove unnecessary services: Unnecessary services can introduce vulnerabilities and be exploited by attackers. Removing them reduces the number of potential attack vectors.

Add the server to the asset inventory: Important for tracking and management but not directly related to hardening.

Document default passwords: Documentation is useful, but changing or disabling default passwords is the hardening step.

Send server logs to the SIEM: Useful for monitoring and analysis but not a direct hardening step. Join the server to the corporate domain: Part of integration into the network but not specific to hardening.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1 - Compare and contrast various types of security controls (Server hardening).

338. A company would like to provide employees with computers that do not have access to the internet in order to prevent information from being leaked to an online forum.

Which of the following would be best for the systems administrator to implement?

- A. Air gap
- B. Jump server
- C. Logical segmentation
- D. Virtualization

Answer: A

Explanation:

To provide employees with computers that do not have access to the internet and prevent information leaks to an online forum, implementing an air gap would be the best solution. An air gap physically isolates the computer or network from any outside connections, including the internet, ensuring that data cannot be transferred to or from the system.

Air gap: A security measure that isolates a computer or network from the internet or other networks, preventing any form of electronic communication with external systems.

Jump server: A secure server used to access and manage devices in a different security zone, but it does not provide isolation from the internet.

Logical segmentation: Segregates networks using software or network configurations, but it does not guarantee complete isolation from the internet.

Virtualization: Creates virtual instances of systems, which can be isolated, but does not inherently prevent internet access without additional configurations.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5 - Explain the purpose of mitigation techniques used to secure the enterprise (Air gap).