Security+ Master Deck Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. Visit https://secplusmasterdeck.examzify.com

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. What type of control is applied when a device uses 128-bit keys instead of the required 256-bit keys due to performance issues?

A. Preventive

B. Corrective

C. Compensating

D. Detective

2. What is one common measure for ensuring security when sharing sensitive information?

A. Using unencrypted email

B. Implementing strong passwords

C. Employing end-to-end encryption

D. Relying solely on user training

3. Which motivation is least likely associated with advanced persistent threat (APT) actors?

A. Financial gain

B. Espionage

C. Ethical

D. Political motives

4. When connecting to an unsecure wired network, which threat is least likely to be a concern?

A. Man-in-the-middle attacks

B. Evil twins

C. Packet sniffing

D. Data encryption

5. What likely occurred if domain information was changed without the domain expiring?

A. Domain hijacking

B. Domain renewal

C. Domain reselling

D. Domain expiration

6. How many keypairs are needed for four individuals to securely communicate using asymmetric encryption?

A. 2

B. 3

C. 4

D. 8

7. What type of attack is characterized by malware flooding a network with packets to an external target?

A. Phishing

B. Man-in-the-middle

C. DDoS

D. Credential stuffing

8. What is the main goal of a DDoS attack?

A. Stealing sensitive information

B. Disrupting services of a targeted server

C. Gaining unauthorized access

D. Infecting a network with malware

9. Which method allows for the tracking and management of changes in system configurations?

A. Version control

B. Static analysis

C. Penetration testing

D. Risk analysis

10. Rick's cloud provider offers a dedicated hardware security module. Which of the following capabilities is it unlikely to offer?

A. Managing encryption keys

B. Validating secure boot processes

C. Performing cryptographic operations

D. Providing secure network connections

Answers

1. C
2. C
3. C
4. D
5. A
6. C
7. C
8. B
9. A
10. B

Explanations

1. What type of control is applied when a device uses 128-bit keys instead of the required 256-bit keys due to performance issues?

A. Preventive

B. Corrective

C. Compensating

D. Detective

In this scenario, when a device opts to use 128-bit keys instead of the required 256-bit keys because of performance issues, it illustrates the concept of compensating controls. Compensating controls are alternative measures that are put in place to mitigate risk when the preferred or ideal security controls cannot be applied due to practical constraints, such as performance. Using 128-bit keys provides a level of security, though it is less robust than the 256-bit keys that were originally required. This change is made as a workaround to maintain operational functionality while still addressing security needs to some extent. Compensating controls aim to provide a balance between security and usability, recognizing that sometimes, ideal security measures cannot be fully implemented. In contrast, preventive controls are meant to prevent security breaches before they occur, corrective controls focus on correcting issues after they have been identified, and detective controls are tasked with identifying security incidents as they happen. However, the use of reduced key lengths due to performance concerns does not directly fit into those categories as it represents a decision to maintain a level of operation that might compromise the ideal standard. Thus, opting to use a less secure key length while still striving to protect data through an alternative measure is why this scenario reflects compensating controls.

2. What is one common measure for ensuring security when sharing sensitive information?

A. Using unencrypted email

B. Implementing strong passwords

C. Employing end-to-end encryption

D. Relying solely on user training

When sharing sensitive information, employing end-to-end encryption is a highly effective security measure. End-to-end encryption ensures that data is encrypted on the sender's device and only decrypts on the recipient's device. This means that even if the data is intercepted while in transit, it remains unreadable to any unauthorized parties. The encryption keys are typically only accessible to the communicating users, adding a robust layer of protection against eavesdropping and interception. This method is particularly crucial in environments where sensitive data—such as personal information, financial transactions, or proprietary business information—requires protection from potential threats during transmission. By using end-to-end encryption, organizations can maintain confidentiality and integrity of the information being shared, effectively mitigating the risks associated with data breaches and unauthorized access.

3. Which motivation is least likely associated with advanced persistent threat (APT) actors?

A. Financial gain

B. Espionage

C. Ethical

D. Political motives

Advanced persistent threat (APT) actors are primarily characterized by their sophisticated techniques, extended engagement, and specific objectives that often align with significant strategic interests. Their motivations typically revolve around financial gain, espionage for obtaining sensitive information, and political objectives that can influence national or organizational power dynamics. When considering ethical motivations, it is crucial to recognize that APT actors do not operate under the principles of ethics as understood in a conventional sense. Instead, they engage in prolonged and covert operations focused on achieving their ends without regard for the ethical implications of their actions. Ethical motives imply a basis for action that is aligned with moral principles or social standards, which is not characteristic of APT operations that prioritize their strategic goals over ethical considerations. Thus, ethical motivation stands apart as the least likely driver for APT actors, who are more often associated with the other mentioned motivations that correspond to their tactical, strategic, and harmful objectives.

4. When connecting to an unsecure wired network, which threat is least likely to be a concern?

A. Man-in-the-middle attacks

B. Evil twins

C. Packet sniffing

D. Data encryption

In the context of connecting to an unsecured wired network, data encryption is least likely to be a concern because encryption typically relates to the protection of data in transit or at rest. In unsecured environments, such as public or poorly secured wired networks, the primary threats involve direct interception and manipulation of data by malicious individuals. Man-in-the-middle attacks, evil twins, and packet sniffing represent active or passive threats that exploit the vulnerabilities of an unsecure network. For instance, a man-in-the-middle attack can occur when an attacker intercepts communications between two parties. Evil twin threats, while more commonly associated with wireless networks, might also apply if a rogue device mimics legitimate network services. Packet sniffing refers to the ability to capture and analyze network traffic, allowing attackers to glean sensitive information. In contrast, data encryption is a defensive measure intended to protect information, and while it is essential for safeguarding data during transmission or storage, its absence is what heightens concern in this type of network. If encryption is not employed, data traveling over the network is inherently vulnerable, but in this context, the existence of encryption is what defines a potential concern rather than a direct threat like those listed.

5. What likely occurred if domain information was changed without the domain expiring?

A. Domain hijacking

B. Domain renewal

C. Domain reselling

D. Domain expiration

If domain information was changed without the domain expiring, this situation most likely indicates domain hijacking. Domain hijacking refers to unauthorized changes made to the registration of a domain name, typically by gaining access to the domain registrar or the associated account. This can happen through various attack vectors, such as phishing or exploiting weak security practices in the account management process. In scenarios involving domain hijacking, the original domain owner may lose control over their domain due to the unauthorized changes made by a malicious actor. This can result in various repercussions, such as traffic redirection, loss of brand identity, and potential financial implications. Meanwhile, other options like domain renewal or expiration do not account for unauthorized changes; they typically involve legitimate processes that the registered owner would undertake. Domain reselling implies that the current owner is intentionally selling the domain, which would not involve unauthorized changes. Thus, the presence of changed domain information without expiration points specifically to the risk associated with domain hijacking.

6. How many keypairs are needed for four individuals to securely communicate using asymmetric encryption?

A. 2

B. 3

C. 4

D. 8

In asymmetric encryption, each individual requires a unique keypair consisting of a public key and a private key. This mechanism allows for secure communication where one person can encrypt data using the other person's public key, and only the intended recipient can decrypt it using their private key.   For four individuals to communicate securely with one another, each individual must possess their own keypair. Therefore, when calculating the number of keypairs needed for four individuals, we simply multiply the number of individuals by the keypairs required per individual. Each of the four individuals requires one keypair, leading to a total of four keypairs needed.   The other choices do not adequately represent the number of keypairs needed for secure communication among four individuals; they either underestimate or overestimate the requirement by not accounting for the necessity of a unique keypair for each participant. Thus, the correct understanding is that each of the four individuals requires one keypair, resulting in a total of four keypairs.

7. What type of attack is characterized by malware flooding a network with packets to an external target?

A. Phishing

B. Man-in-the-middle

C. DDoS

D. Credential stuffing

The type of attack characterized by malware flooding a network with packets to an external target is known as a Distributed Denial of Service (DDoS) attack. In a DDoS attack, multiple compromised systems are leveraged to launch a coordinated assault on a single target—such as a server or network. This overwhelming volume of requests forces the target to become unresponsive or extremely slow, effectively denying legitimate users access to the service. DDoS attacks typically involve a botnet, which is a network of infected devices under the control of an attacker. These devices, roused by malicious software, send vast amounts of traffic towards the intended target, resulting in a saturation of its resources. This method is distinct from other forms of attacks like phishing, which seeks to deceive individuals into providing sensitive information, or man-in-the-middle attacks, which intercept and alter communications between two parties. Credential stuffing pertains to the use of stolen usernames and passwords to gain unauthorized access to user accounts, rather than overwhelming systems with traffic. In summary, DDoS attacks specifically focus on disrupting the availability of services through massive traffic generation, distinguishing them from other attack types.

8. What is the main goal of a DDoS attack?

A. Stealing sensitive information

B. Disrupting services of a targeted server

C. Gaining unauthorized access

D. Infecting a network with malware

The primary goal of a Distributed Denial of Service (DDoS) attack is to disrupt services of a targeted server. This type of attack overwhelms the resources of the target, making it impossible for legitimate users to access services or information. By flooding the target server with an excessive amount of traffic, the attackers effectively incapacitate the system, leading to downtime and lost functionality.   DDoS attacks specifically aim to create service unavailability rather than obtaining sensitive information, gaining unauthorized access, or infecting a network with malware. While other forms of cyber attacks may focus on those aspects, the distinct characteristic of a DDoS attack is its objective to render a service or network resource completely unreachable for its users, causing inconvenience and potential financial loss.

9. Which method allows for the tracking and management of changes in system configurations?

A. Version control

B. Static analysis

C. Penetration testing

D. Risk analysis

Version control is the method that facilitates the tracking and management of changes in system configurations. It is commonly used in software development and IT management to maintain multiple versions of system files, allowing teams to see what changes were made, by whom, and when. This capability is crucial for troubleshooting, collaboration, and ensuring system integrity over time. When system configurations undergo changes, version control helps maintain a history of those changes, making it easier to revert to previous states if necessary, thus enhancing overall stability and security. Static analysis pertains to examining code without executing it, primarily to find bugs or vulnerabilities before the software is run. This method does not involve the systematic tracking of configuration changes over time. Penetration testing is a technique used to identify vulnerabilities within systems by simulating attacks. While it helps assess security postures, it does not provide a framework for managing or tracking changes in system configurations. Risk analysis involves evaluating potential risks that could impact the organization's information systems but does not directly focus on change management or configuration tracking. In summary, version control is the most appropriate method for effective tracking and management of changes in system configurations, ensuring that IT systems remain consistent and secure over time.

10. Rick's cloud provider offers a dedicated hardware security module. Which of the following capabilities is it unlikely to offer?

A. Managing encryption keys

B. Validating secure boot processes

C. Performing cryptographic operations

D. Providing secure network connections

A dedicated hardware security module (HSM) primarily focuses on the management of cryptographic keys and performing cryptographic operations securely, which involves physical security and tamper resistance to protect sensitive operations and information. Managing encryption keys is a core function of HSMs, allowing them to generate, store, and handle encryption keys in a secure environment, making this capability inherently aligned with their primary purpose. HSMs are designed to perform cryptographic operations, which encompass tasks such as encryption, decryption, and digital signing, leveraging the module's secure processing environment. Providing secure network connections, while possibly assisted by HSM capabilities, falls more into the realm of networking and security protocols rather than being a direct function of an HSM. While an HSM can be used in conjunction with secure communications, it does not directly create or manage network connections itself. Validating secure boot processes is generally not a task performed by an HSM. Secure boot validation often relies on establishing a trusted computing base, which may involve various software and firmware checks—functions that are typically outside the specialized scope of a hardware security module. Instead, secure boot is more about ensuring that the startup process of a device runs only trustworthy software, which is not the primary function of an