Cisco Cyber Security Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Which of the following is NOT a primary function of an IPS?

A. Quarantine infected systems

B. Log network traffic

C. Monitor user activities

D. Detect and respond to threats

2. Which hashing algorithm can produce hash values beyond 128 bits?

A. MD5

B. SHA

C. DES

D. RC4

3. What is the responsibility of a data processor?

A. To classify data assets

B. To implement security measures

C. To process personal data on behalf of the data controller

D. To ensure compliance with laws

4. In cryptography, what is typically used to ensure data integrity?

A. Encryption

B. Hashing

C. Compression

D. Obfuscation

5. What non-technical method could a cybercriminal use to gather sensitive information from an organization?

A. Phishing

B. Social Engineering

C. Malware

D. Hacking

6. What type of control is implemented when a warning banner is displayed about the negative outcomes of breaking company policy?

A. Preventive

B. Deterrent

C. Corrective

D. Compensating

7. Which of the following is NOT a function of a stateful firewall?

A. Tracking active connections

B. Filtering based on IP addresses only

C. Monitoring connection establishment

D. Allowing or denying based on session state

8. Which factor should cybersecurity professionals understand to make informed ethical decisions regarding sensitive data?

A. Industry standards

B. Regulatory compliance

C. Laws governing the data

D. Organizational policies

9. What type of VPN is likely being used if web pages and video streaming are slow for a remote team member?

A. A split VPN tunnel

B. A full VPN tunnel

C. A mobile VPN

D. A client-to-site VPN

10. What can the input to a hash function be in terms of length?

A. Fixed length

B. Any length

C. Preferred length

D. Standard length

Answers

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

Explanations

1. Which of the following is NOT a primary function of an IPS?

A. Quarantine infected systems

B. Log network traffic

C. Monitor user activities

D. Detect and respond to threats

An Intrusion Prevention System (IPS) is primarily focused on the detection and prevention of intrusion attempts in a network environment. Among its core functions are detecting and responding to threats, logging network traffic for analysis, and, in some contexts, taking action to quarantine infected systems to prevent further infection. Monitoring user activities, while it may be an aspect of broader security practices, is not a primary function of an IPS. This task typically falls under user behavior analytics or other systems focused on monitoring user actions for compliance or suspicious activity, rather than being a direct responsibility of an IPS. An IPS's main goals are around threat detection and immediate response to potential intrusions rather than detailed user activity monitoring.

2. Which hashing algorithm can produce hash values beyond 128 bits?

A. MD5

B. SHA

C. DES

D. RC4

The choice of SHA as the hashing algorithm that can produce hash values beyond 128 bits is accurate as SHA (Secure Hash Algorithm) encompasses a range of algorithms with varying output lengths. Specifically, SHA-1 generates a 160-bit hash, SHA-256 produces a 256-bit hash, and SHA-512 creates a 512-bit hash. This variability allows SHA algorithms to be used in applications requiring higher security standards, as longer hash values generally provide increased resistance against collision attacks. In contrast, MD5 is limited to a 128-bit hash output, making it susceptible to vulnerabilities that can be exploited to produce identical hash outputs from different inputs. DES (Data Encryption Standard) is not a hashing algorithm; it is a symmetric-key block cipher used for encryption rather than hashing, which does not produce hash values at all. Similarly, RC4 is a stream cipher used for encryption and does not generate hash values, further distinguishing it from proper hashing algorithms like SHA. Thus, the choice of SHA is the most fitting, given its ability to produce hash values exceeding 128 bits.

3. What is the responsibility of a data processor?

A. To classify data assets

B. To implement security measures

C. To process personal data on behalf of the data controller

D. To ensure compliance with laws

The responsibility of a data processor is to process personal data on behalf of the data controller. This role involves handling and managing data that has been entrusted to them by the data controller, who determines the purposes and means of processing such data. The data processor acts under the instructions of the data controller and must carry out processing activities as specified in a contractual agreement. This can include tasks such as storing, managing, or analyzing data without having the authority to make decisions on how the data can be used. The relationship between data controllers and data processors is crucial within data protection and privacy frameworks, such as the General Data Protection Regulation (GDPR). The data processor must ensure that the processing is conducted in a manner that complies with the contractual obligations set forth by the data controller, and they may also have specific obligations to aid the controller in meeting compliance requirements regarding data protection laws.

4. In cryptography, what is typically used to ensure data integrity?

A. Encryption

B. Hashing

C. Compression

D. Obfuscation

Hashing is primarily used to ensure data integrity in cryptography. When data is hashed, a fixed-size output known as a hash value or digest is produced from input data of any size. Even the slightest change in the original data—whether it's an added character or a modified byte—results in a significantly different hash value. This property is called the avalanche effect, and it makes hashes useful for verifying that data has not been altered. When data integrity is essential, such as in transmitting files over a network or storing sensitive information, a system can generate a hash value of the original data. Upon receipt or retrieval, the system computes the hash value of the data again and compares it with the original. If the two hash values match, it confirms that the data remains unchanged and intact. If they differ, it indicates that the data may have been tampered with or corrupted. While encryption also serves a purpose in securing data, its primary function is confidentiality, protecting against unauthorized access rather than ensuring that the data has not been modified. Compression reduces the size of data but does not provide any guarantees about its integrity. Obfuscation involves making data unclear or unintelligible, often to protect intellectual property or sensitive information, but it does not maintain data integrity

5. What non-technical method could a cybercriminal use to gather sensitive information from an organization?

A. Phishing

B. Social Engineering

C. Malware

D. Hacking

Social engineering is a non-technical method used by cybercriminals to deceive individuals into divulging confidential or sensitive information. This approach relies on manipulating human psychology rather than exploiting technical vulnerabilities. Cybercriminals may employ tactics such as impersonating authority figures, using psychological tricks to create a sense of urgency, or establishing trust to encourage victims to share personal information, passwords, or access credentials. In the context of security, while phishing does involve deceptive tactics to collect sensitive information, it is typically executed through electronic communication, making it a more technical method compared to social engineering. Other terms like malware and hacking refer to technical approaches that involve software and system vulnerabilities, whereas social engineering emphasizes the interpersonal interaction aspect. This distinction is what makes social engineering noteworthy as a non-technical method for information gathering.

6. What type of control is implemented when a warning banner is displayed about the negative outcomes of breaking company policy?

A. Preventive

B. Deterrent

C. Corrective

D. Compensating

Displaying a warning banner about the negative outcomes of breaking company policy serves as a deterrent control. Deterrent controls are designed to discourage individuals from engaging in undesirable behaviors or actions by making them aware of the consequences. In this case, the warning banner informs employees of the potential negative repercussions they may face if they violate company policy, such as disciplinary actions or legal consequences. This awareness can influence their decisions and behavior, steering them away from actions that could jeopardize security or compliance. Preventive controls, on the other hand, are aimed at stopping a security incident before it occurs, such as firewalls or access controls. Corrective controls take action after an incident has occurred to restore systems or data to a previous state, while compensating controls provide an alternative means to meet security requirements when primary controls are not feasible. The purpose of the warning banner aligns specifically with the deterrent approach by promoting a culture of compliance and awareness rather than merely implementing barriers or remedies after the fact.

7. Which of the following is NOT a function of a stateful firewall?

A. Tracking active connections

B. Filtering based on IP addresses only

C. Monitoring connection establishment

D. Allowing or denying based on session state

A stateful firewall is designed to keep track of the state of active connections and make decisions based on the context of traffic flows. Its primary functions include tracking active connections, monitoring connection establishment and termination, and allowing or denying traffic based on the current state of the session. Filtering based solely on IP addresses, however, is characteristic of a stateless firewall. Stateless firewalls evaluate packets in isolation, meaning they do not maintain any internal record of the state of network connections. Therefore, their filtering capabilities are limited to criteria such as IP addresses and port numbers without considering the overall context of the communication session. In contrast, a stateful firewall incorporates session information, enhancing security by allowing it to differentiate between legitimate returning traffic and potential threats. This understanding underscores why filtering based solely on IP addresses is not a function of a stateful firewall, as it would not utilize the benefits of connection tracking that stateful firewalls offer.

8. Which factor should cybersecurity professionals understand to make informed ethical decisions regarding sensitive data?

A. Industry standards

B. Regulatory compliance

C. Laws governing the data

D. Organizational policies

Understanding the laws governing data is crucial for cybersecurity professionals when making informed ethical decisions about sensitive data. Laws provide the framework that dictates how data must be collected, handled, stored, and shared. They define the rights of individuals regarding their data and outline the responsibilities of organizations in protecting that data. For instance, laws such as the General Data Protection Regulation (GDPR) in Europe or the Health Insurance Portability and Accountability Act (HIPAA) in the United States establish specific legal obligations for data protection and privacy. This legal knowledge enables professionals to ensure that their actions are compliant with the requirements and expectations set forth by legislation. It also helps them navigate complex situations where ethical implications may arise, ensuring that decisions align not only with best practices but also with legal standards. In scenarios involving sensitive data, being aware of the legal ramifications can prevent breaches, protect individuals' rights, and uphold the organization's integrity. Nevertheless, industry standards, regulatory compliance, and organizational policies are also significant considerations in this context. While they contribute to the overarching framework for managing data, they often function within the boundaries defined by laws. Therefore, a solid understanding of the legal framework is essential to effectively interpret and apply these other factors in ethical decision-making.

9. What type of VPN is likely being used if web pages and video streaming are slow for a remote team member?

A. A split VPN tunnel

B. A full VPN tunnel

C. A mobile VPN

D. A client-to-site VPN

A full VPN tunnel is likely being used if web pages and video streaming are slow for a remote team member. In a full VPN tunnel, all traffic from the user's device is routed through the VPN server, which can lead to slower performance due to several factors such as increased latency from the additional routing, potential bandwidth limitations of the VPN server, and encryption overhead. When all internet traffic, including standard web browsing and streaming, is encrypted and sent through the VPN, it results in a bottleneck effect, particularly if the VPN server has limited resources or if there are many users connected simultaneously. In contrast, a split VPN tunnel allows certain traffic to bypass the VPN, maintaining performance for regular internet browsing and streaming by allowing them to connect directly to the internet. Mobile VPNs typically focus on providing secure connectivity while on the move, and client-to-site VPNs describe a specific architecture for secure connections from individual clients to a corporate network, which may not necessarily affect performance in the same way. Thus, slow performance in web browsing and video streaming suggests that the remote user is experiencing the effects of a full VPN tunnel.

10. What can the input to a hash function be in terms of length?

A. Fixed length

B. Any length

C. Preferred length

D. Standard length

The input to a hash function can be of any length, making it versatile for various applications. This means that irrespective of how large or small the input data is, the hash function can process it. When you provide data to a hash function, it processes the input, regardless of its size, and produces a fixed-length output, typically referred to as the hash value or digest. This characteristic of accepting any length is crucial because it allows for the hashing of data such as files, messages, or any forms of input that can vary significantly in size. For instance, whether the input is a short password or a lengthy document, the hash function will still generate a consistent sized output. This fixed output length provides benefits for data integrity and security, as it ensures that the hashes can be easily compared, stored, and utilized regardless of the input size. The other choices imply restrictions on the input length, which do not align with the fundamental principles of how hash functions operate. By allowing inputs of any length, hash functions serve a broader range of processes in cryptography and data integrity checks.