CERT QUEEN

100-160

Exam Name: Cisco Certified Support Technician (CCST) Cybersecurity

Full version: 309 Q&As

[Full version of 100-160 Dumps]

Share some 100-160 exam dumps below.

1. What is the purpose of encryption in network security?

A. To monitor and detect network attacks

B. To authenticate and authorize users

C. To protect the confidentiality and integrity of data during transmission

D. To prevent unauthorized physical access to network devices

Answer: C

Explanation:

Encryption is the process of transforming data into an unintelligible form (ciphertext) to protect its confidentiality and integrity during transmission. It ensures that even if the data is intercepted, it cannot be understood or modified without the encryption key. Encryption helps in safeguarding sensitive information from unauthorized access and tampering.

2. Which of the following best describes the concept of defense in depth in cybersecurity?

A. Utilizing multiple layers of security controls to protect against different types of threats

B. Running regular vulnerability scans to maintain the integrity of the system

C. Implementing access controls to ensure availability of critical resources

D. Encrypting sensitive data to maintain confidentiality

Answer: A

Explanation:

Defense in depth is a cybersecurity strategy that involves implementing multiple layers of security controls to protect against various types of threats. This approach provides greater resilience and mitigates potential vulnerabilities. By implementing multiple layers, even if one control fails, others can still safeguard the system.

3. Which compliance framework lays out guidelines for protecting the privacy of student education records in educational institutions?

A. HIPAA

B. PCI-DSS

C. FERPA

D. GDPR

Answer: C

Explanation:

The Family Educational Rights and Privacy Act (FERPA) is a compliance framework that safeguards the privacy of student education records in educational institutions. FERPA provides guidelines for the control and release of these records, ensuring that students' personally identifiable information (PII) is protected and not disclosed without consent.

4. Which of the following is an example of a preventive control?

A. Incident response plan

B. User access log

C. Firewall

D. Intrusion detection system

Answer: C

Explanation:

A firewall is a preventive control that helps to protect a network by acting as a barrier between internal and external networks, monitoring and controlling incoming and outgoing traffic based on predetermined security rules. It prevents unauthorized access and defends against network-based attacks.

5. Which protocol is commonly used for remote user authentication and authorization?

A. TACACS+

B. RADIUS

C. LDAP

D. SSH

Answer: B

Explanation:

RADIUS (Remote Authentication Dial-In User Service) is a widely-used protocol for remote user authentication and authorization. It provides centralized authentication, authorization, and accounting management for users who dial in or connect remotely to a network. RADIUS uses a client-server model where the client (network access server) forwards user authentication requests to the RADIUS server for validation.

6. Why are data backups important in a cybersecurity strategy?

A. To recover from physical hardware failures

B. To prevent unauthorized access to sensitive information

C. To analyze historical data for identifying security incidents

D. To track changes made to critical system files

Answer: A

Explanation:

Data backups are essential in a cybersecurity strategy primarily to ensure the ability to recover from physical hardware failures, such as server crashes, disk failures, or natural disasters. Regularly backing up critical data helps organizations restore their systems and resume normal operations in case of hardware failures or any other catastrophic events that may result in data loss.

7. Which of the following is an example of a data security principle?

A. Least Privilege

B. Session Management

C. ARP Spoofing

D. Ciphertext

Answer: A

Explanation:

Option 1: Correct. Least Privilege is a data security principle that limits the access rights of individuals to only what is necessary for them to perform their job functions.

Option 2: Incorrect. Session Management is a security practice related to handling user sessions, but it is not specifically a data security principle.

Option 3: Incorrect. ARP Spoofing is a network attack technique, not a data security principle.

Option 4: Incorrect. Ciphertext refers to encrypted data, but it is not a data security principle.

8. Which of the following is a primary purpose of software inventory in a cybersecurity program?

A. Monitoring user access and permissions

B. Identifying vulnerabilities and patch requirements

C. Analyzing network traffic for potential threats

D. Ensuring compliance with software licensing agreements

Answer: B

Explanation:

Software inventory is an essential component of a cybersecurity program as it helps in identifying the software applications installed on devices within the network. By maintaining an accurate software inventory, organizations can identify vulnerabilities and track patch requirements to keep their systems secure and up to date.

9. Which of the following is an example of a network vulnerability?

A. Encrypting sensitive data

B. Running outdated and unpatched software

C. Using a strong password

D. Implementing a firewall

Answer: B

Explanation:

Running outdated and unpatched software is an example of a network vulnerability. Software updates often include patches to fix security vulnerabilities that have been discovered. Failing to install these updates or using outdated software increases the risk of an attacker exploiting known vulnerabilities to gain unauthorized access or compromise the network.

10. Which of the following best describes the purpose of the MITRE ATT&CK; Matrix?

A. To map vulnerabilities and exposures in computer systems

B. To analyze the impact of cyber threats on critical infrastructure

C. To track the global distribution of cyber threat actors

D. To provide a standardized way to categorize cyber threat tactics and techniques

Answer: D

Explanation:

The MITRE ATT&CK; Matrix provides a comprehensive framework that categorizes various tactics, techniques, and procedures (TTPs) used by cyber threat actors. It enables organizations to understand how different attackers operate and helps in developing effective cybersecurity defenses and detection mechanisms.

11. What is a digital certificate used for in the context of cybersecurity?

A. Encrypting data

B. Verifying the identity of an entity

C. Creating a secure tunnel

D. Decrypting data

Answer: B

Explanation:

A digital certificate is an electronic document used to prove the authenticity and identity of an entity, such as a person, organization, or device, in an online environment. It is issued and digitally signed by a trusted third party known as a certification authority (CA). Digital certificates are commonly used in cybersecurity for purposes such as authentication, ensuring secure communication, and establishing trust between entities.

12. What is encryption?

A. A process of converting plaintext into binary code to enhance data accessibility

B. A process of converting binary code into plaintext to improve data reliability

C. A process of converting plaintext into ciphertext to protect data confidentiality

D. A process of converting ciphertext into plaintext to secure data integrity

Answer: C

Explanation:

Encryption is the process of converting plaintext (original data) into a coded or unreadable format known as ciphertext. This ensures that if the data is intercepted or accessed by unauthorized individuals, they would not be able to understand the information without the appropriate decryption key. Encryption is used to protect the confidentiality and privacy of sensitive data during transmission or storage.

13. Which encryption method is used to secure data while it is being actively used and processed by an application?

A. Asymmetric encryption

B. Homomorphic encryption

C. Secure Sockets Layer (SSL)

D. Hash encryption

Answer: B

Explanation:

Homomorphic encryption is a form of encryption that allows computations to be performed on encrypted data without decrypting it. This method enables the secure processing and manipulation of data while it is in use by an application or system. Homomorphic encryption is particularly useful in scenarios where privacy is a concern, such as in cloud computing or data analytics.

14. Which state of data is appropriate for encrypting sensitive information stored in a database?

A. Data in motion

B. Data in transit

C. Data at rest

D. Data in use

Answer: C

Explanation:

Data at rest refers to data that is stored on storage devices such as hard drives, databases, or backups. Encrypting sensitive information in a database while it is at rest ensures that even if the database is compromised, the data remains protected, and unauthorized access or theft of the data becomes more challenging.

15. Which type of encryption protects data while it is being transmitted over a network?

A. Transport Layer Security (TLS)

B. Asymmetric encryption

C. Symmetric encryption

D. Hash encryption

Answer: A

Explanation:

Transport Layer Security (TLS) is a cryptographic protocol that provides secure communication over a network. It ensures the confidentiality and integrity of data while in transit by encrypting it. TLS is commonly used to protect sensitive information during online transactions, such as credit card numbers or login credentials.

16. Which of the following best defines risk management in the context of cybersecurity?
A. The process of analyzing potential threats and determining the likelihood and impact of those threats on an organization.
B. The process of ensuring the confidentiality, integrity, and availability of an organization's information assets.
C. The process of mitigating threats to an organization's information assets by implementing appropriate security controls.
D. The process of identifying, assessing, and prioritizing vulnerabilities in an organization's networks
and systems.
Answer: A
Explanation:
Risk management is the process of identifying, assessing, and prioritizing potential threats to an organization's information assets. By analyzing the likelihood and impact of these threats, organizations can make informed decisions on how to mitigate risks effectively. This process involves activities such as risk assessment, risk analysis, risk mitigation, and risk monitoring. The focus is on evaluating the probability and impact of potential cybersecurity incidents and implementing appropriate measures to reduce or eliminate these risks.

17. Which of the following is an example of a corrective control?
A. Antivirus software
B. User awareness training
C. Intrusion prevention system
D. Backup and recovery
Answer: D
Explanation:
Backup and recovery is a corrective control that enables organizations to restore systems, data, and services after an incident or a failure. It helps to recover from various incidents such as data loss, hardware failure, or a security breach, restoring operations to a functional state.

18. Which of the following best defines vulnerability management?

A. An approach to monitor and analyze network traffic for security threats.

B. A technique used to encrypt data while in transit over a network.

C. A process of identifying, classifying, and mitigating vulnerabilities in a system or network.

D. A method to detect and respond to unauthorized access attempts on a system.

Answer: C

Explanation:

Vulnerability management is the practice of systematically identifying, categorizing, and addressing vulnerabilities in a system or network. It involves activities such as vulnerability scanning, vulnerability assessment, and vulnerability remediation. The goal of vulnerability management is to minimize the risk of potential exploits by proactively identifying and addressing security weaknesses.

19. Which of the following describes the purpose of a firewall in network infrastructure?

A. To provide high-speed connectivity between different networks

B. To monitor network traffic for potential security threats

C. To regulate the flow of data between different network segments

D. To identify and prevent unauthorized access to the network

Answer: C

Explanation:

A firewall is a network security device that is designed to monitor and control the incoming and outgoing network traffic. It acts as a barrier between different network segments, regulating the flow of data according to predefined security policies. Firewalls help to prevent unauthorized access to the network by allowing only authorized traffic and blocking any potentially harmful traffic.

20. Which of the following is an important step during the containment phase of incident handling?

A. Preserving evidence for forensic investigation

B. Notifying law enforcement agencies

C. Implementing temporary workarounds to mitigate the impact

D. Identifying the root cause of the incident

Answer: C

Explanation:

Implementing temporary workarounds to mitigate the impact is an important step during the containment phase of incident handling. This step aims to limit the further spread or damage caused by the incident while the root cause is being investigated and fully addressed. While notifying law enforcement, preserving evidence, and identifying the root cause are all important, the immediate focus should be on minimizing the impact of the incident.

21. Which of the following is an example of a human-caused disaster?
A. Tornado
B. Flood
C. Earthquake
D. Cyberattack
Answer: D
Explanation:
Cyberattacks, such as hacking, malware, or ransomware attacks, are considered human-caused disasters. They are intentional actions carried out by individuals or groups with malicious intent and can result in significant disruption, data loss, and financial damage if proper cybersecurity measures are not in place.

22. Which of the following is a best practice for proactively managing and securing communication before, during, and after an event?
A. Limiting access to essential personnel only
B. Conducting regular security audits
C. Regularly updating antivirus software
D. Encrypting sensitive data at rest and in transit
Answer: D
Explanation:
Encrypting sensitive data at rest and in transit is a best practice for securing communication before, during, and after an event. Encryption ensures that data is encoded in a way that only authorized parties can access and understand it. By encrypting sensitive data, even if it is intercepted by unauthorized individuals, they would not be able to make sense of the information without the encryption key, thus maintaining its confidentiality and integrity during transmission and storage.

23. What is the purpose of Security Information and Event Management (SIEM) systems?
A. To analyze network traffic and detect potential security threats.
B. To centrally collect, store, and analyze logs from various systems to detect and respond to security incidents.
C. To encrypt sensitive data to protect it from unauthorized access.
D. To authenticate and authorize users to access network resources.

Answer: B

Explanation:

Option 1: This option is incorrect. While SIEM systems may perform analysis of network traffic, their primary purpose is not network traffic analysis, but rather log collection and analysis for security incident detection and response.

Option 2: This option is correct. SIEM systems are designed to centrally collect, store, and analyze logs from various systems to detect and respond to security incidents. They provide real-time monitoring, correlation, and analysis of security events, allowing organizations to identify potential threats and take appropriate actions.

Option 3: This option is incorrect. Encryption of sensitive data is not the purpose of SIEM systems. While encryption is an important security measure, SIEM systems focus on log management and analysis rather than encryption.

Option 4: This option is incorrect. User authentication and authorization are not within the scope of SIEM systems. SIEM systems focus on log collection and analysis for security incident detection and response, rather than user access control.

24. What is the primary purpose of a VPN (Virtual Private Network)?

A. To encrypt email communications

B. To secure wireless network connections

C. To establish a secure remote connection over a public network

D. To protect against malware attacks

Answer: C

Explanation:

A VPN is designed to provide secure, encrypted communication over a public network such as the internet. Its primary purpose is to establish a secure and private connection between two endpoints, allowing remote users to access resources on a private network as if they were directly connected to it. This helps protect sensitive data and communications from interception by unauthorized individuals.

25. Which protocol is used for broadcasting and resolving MAC addresses to IP addresses?

A. ICMP

B. TCP

C. ARP

D. UDP

Answer: C

Explanation:

ARP (Address Resolution Protocol) is used for broadcasting and resolving MAC (Media Access Control) addresses to IP addresses within a local network. It helps devices determine the MAC address associated with a given IP address, enabling proper communication on the network. ARP operates at the data link layer of the OSI model.

26. Which of the following is a network security device that operates at the session layer of the OSI model?

A. Firewall

B. Intrusion Detection System (IDS)

C. Intrusion Prevention System (IPS)

D. SSL/TLS

Answer: B

Explanation:

Option 1: Incorrect. A firewall operates at the network layer (layer of the OSI model, not the session layer (layer 5).

Option 2: Correct. An Intrusion Prevention System (IPS) operates at the session layer (layer 5) of the OSI model. It monitors network traffic in real-time and can block or prevent malicious activities.

Option 3: Incorrect. An Intrusion Detection System (IDS) operates at the network layer (layer of the OSI model, not the session layer (layer 5).

Option 4: Incorrect. SSL/TLS is a cryptographic protocol that operates at the transport layer (layer of the OSI model, not the session layer (layer 5).

27. Which of the following is an example of a detective control?

A. Security information and event management (SIEM) system

B. Access control list (ACL)

C. Patch management

D. Encryption

Answer: A

Explanation:

A SIEM system is a detective control that collects and analyzes security event logs from various sources to identify and detect potential security incidents. It provides real-time monitoring and alerts for suspicious activities, enabling organizations to identify and respond to security events effectively.

28. Which encryption algorithm is commonly used for securing wireless network

communication?

A. RC4

B. SSL

C. AES

D. DES

Answer: C

Explanation:

AES (Advanced Encryption Standard) is widely used for securing wireless network communications. It is considered a strong and secure symmetric encryption algorithm that provides confidentiality and data integrity in wireless networks. AES has become the standard encryption algorithm for securing Wi-Fi networks (WPA2).

29. Which of the following options is an example of a cybersecurity news and subscription service?

A. VPN (Virtual Private Network)

B. Email filtering software

C. SIEM (Security Information and Event Management) system

D. Firewall

Answer: C

Explanation:

A SIEM system is an example of a cybersecurity news and subscription service. It collects and analyzes security event data from various sources and provides real-time alerts and reports to enhance threat detection and management. It provides valuable insights into the cybersecurity landscape, including news and updates related to security incidents, vulnerabilities, and emerging threats.

30. Which of the following control types is focused on identifying vulnerabilities and weaknesses in systems and addressing them?

A. Preventive controls

B. Compensating controls

C. Detective controls

D. Corrective controls

Answer: D

Explanation:

Corrective controls are designed to identify and rectify vulnerabilities and weaknesses in systems. They aim to correct issues identified through assessments, audits, or incident response, and ensure that the necessary steps are taken to minimize the associated risks. Examples of corrective controls include patch management, vulnerability scanning, and system hardening procedures.

31. Which of the following is an effective strategy for managing communication proactively?
A. Regularly monitoring network traffic
B. Deploying intrusion detection systems
C. Implementing strong access controls
D. Conducting regular vulnerability assessments
Answer: C
Explanation:
Implementing strong access controls is an effective strategy for managing communication proactively. By implementing access controls, organizations can restrict access to communication channels, ensuring that only authorized personnel have the necessary privileges to communicate and access sensitive information. This helps to prevent unauthorized users from intercepting or tampering with communications, reducing the risk of security incidents.

32. What is the purpose of vulnerability management in cybersecurity?
A. To identify and address vulnerabilities in a timely manner.
B. To transfer ownership of cybersecurity risks to third-party vendors.
C. To assess the level of cybersecurity risk associated with a system or network.
D. To mitigate the impact of cybersecurity incidents within an organization.
Answer: A
Explanation:
The purpose of vulnerability management in cybersecurity is to identify, assess, and address vulnerabilities in a timely manner. It involves a systematic approach to scanning, testing, and monitoring for vulnerabilities in systems, networks, and applications. By proactively managing vulnerabilities, organizations can reduce the likelihood of successful cyber-attacks and minimize potential damages. Vulnerability management typically includes processes such as vulnerability scanning, vulnerability patching, and vulnerability remediation.

33. Which regulation sets standards for the security and privacy of protected health information (PHI) in the United States?
A. GDPR
B. BYOD
C. HIPAA

D. PCI DSS

Answer: C

Explanation:

The Health Insurance Portability and Accountability Act (HIPAA) is a regulation in the United States that sets standards for the security and privacy of protected health information (PHI). It applies to organizations, such as healthcare providers, health plans, and healthcare clearinghouses, that handle PHI.

34. What is the purpose of app distribution in cybersecurity?

A. Deploying network firewalls

B. Testing the security of applications

C. Configuring access control policies

D. Distributing security patches and updates

Answer: D

Explanation:

App distribution in cybersecurity refers to the process of distributing security patches and updates for applications. This is vital in maintaining the security of software and preventing vulnerabilities from being exploited. By regularly distributing and installing updates, organizations can address known security flaws, improve application performance, and ensure that their systems remain protected against emerging threats.

35. Why is it important to maintain the chain of custody when handling digital evidence?

A. To accelerate the analysis of the evidence.

B. To prevent unauthorized access or tampering.

C. To ensure the evidence is stored securely.

D. To recover lost or deleted data from the evidence.

Answer: B

Explanation:

Maintaining the chain of custody is crucial to ensure the integrity and admissibility of digital evidence in a legal case. It helps establish that the evidence has not been tampered with or accessed by unauthorized individuals, which ensures its reliability and credibility. By maintaining a strict chain of custody, any potential challenges to the evidence's validity can be effectively addressed by demonstrating that it has been handled in a controlled and secure manner.

36. Which of the following is an example of a network layer (Layer 3) security control?

A. Encryption

B. Intrusion Detection System (IDS)

C. Antivirus software

D. Firewall

Answer: D

Explanation:

A firewall operates at the network layer (Layer 3) of the OSI model and is designed to control incoming and outgoing network traffic based on a set of predetermined security rules. It acts as a barrier between an internal network and external networks, filtering and inspecting packets to prevent unauthorized access and protect against various types of network attacks.

37. Which of the following is a common threat to cybersecurity?

A. Software updates

B. Data encryption

C. User authentication

D. Phishing attacks

Answer: D

Explanation:

Phishing attacks are a common threat to cybersecurity. They involve fraudulent attempts to obtain sensitive information, such as passwords and credit card details, by disguising as a trustworthy entity in electronic communication. It is important to be cautious and verify the authenticity of any requests for personal information to protect against phishing attacks.

38. Which of the following best describes the term "as they occur" in the context of cybersecurity?

A. Planning and executing incident response procedures

B. Developing mitigation strategies for potential security threats

C. Conducting regular security audits and assessments

D. Monitoring and analyzing security events in real-time

Answer: D

Explanation:

"As they occur" refers to the practice of continuously monitoring and analyzing security events as they happen. This involves setting up systems and tools to detect and alert on potential security incidents in real-time. By identifying and addressing security events promptly, organizations can reduce the impact and minimize potential damage.

39. Which encryption method uses a single key to both encrypt and decrypt data?

A. SSL/TLS

B. Symmetric encryption

C. Hashing

D. Asymmetric encryption

Answer: B

Explanation:

Symmetric encryption uses a single key to both encrypt and decrypt data. This means that the same key is used by both the sender and the receiver to secure the communication. It is faster and less computationally intensive than asymmetric encryption.

40. What is the main motivation for attackers to conduct cyber attacks?

A. Knowledge

B. Financial gain

C. Curiosity

D. Revenge

Answer: B

Explanation:

The primary motivation for many cyber attackers is financial gain. By conducting cyber attacks, attackers may aim to steal sensitive information, such as credit card details or personal data, which they can then use or sell for financial profit.

41. What regulation is specifically designed to ensure the security of payment card data processed by organizations?

A. GDPR

B. BYOD

C. PCI DSS

D. HIPAA

Answer: C

Explanation:

The Payment Card Industry Data Security Standard (PCI DSS) is a regulation that focuses on ensuring the security of payment card data processed by organizations. It provides a set of security requirements that organizations handling payment card data must follow to protect against fraud and data breaches.

42. Which of the following is an example of personally identifiable information (PII)?

A. Birthdate

B. Browser history

C. Employee ID number

D. IP address

Answer: A

Explanation:

Personally identifiable information (PII) refers to any data that can be used to identify an individual.

Birthdate is considered PII as it can be used to pinpoint a specific person.

43. Which of the following threat intelligence techniques involves monitoring network traffic and analyzing abnormal patterns or behaviors?

A. Reputation-based Detection

B. Indicators of Compromise (IoCs)

C. Signature-based Detection

D. Anomaly-based Detection

Answer: D

Explanation:

Anomaly-based detection involves monitoring network traffic and comparing it against baseline or normal behavior. It looks for any abnormal patterns or behaviors that could indicate potential threats.

44. Which of the following is a characteristic of weak encryption algorithms?

A. They support secure communication protocols.

B. They are susceptible to cryptanalysis attacks.

C. They are resistant to brute force attacks.

D. They provide encryption keys with longer bit lengths.

Answer: B

Explanation:

Weak encryption algorithms are those that can be easily broken or exploited using various encryption analysis techniques. These algorithms have vulnerabilities that can be used to decrypt the encrypted

data without the need for the encryption key.

45. Which of the following is NOT a benefit of maintaining a hardware inventory?

A. Facilitates asset management and procurement

B. Enhances the effectiveness of software inventory management

C. Simplifies troubleshooting and technical support

D. Eliminates the need for software updates and patching

Answer: D

Explanation:

Maintaining a hardware inventory provides multiple benefits, including simplifying troubleshooting, facilitating asset management, and enhancing software inventory management. However, it does not eliminate the need for software updates and patching, as those are separate activities required to
maintain the security and functionality of software components.

46. Which of the following best describes the purpose of an information security assessment?

A. To identify and mitigate security vulnerabilities and risks

B. To create a comprehensive inventory of IT assets

C. To determine the level of compliance with industry standards and regulations

D. To assess the impact of changes on organizational processes

Answer: A

Explanation:

An information security assessment is performed to evaluate the security posture of an IT system. Its main purpose is to identify and mitigate security vulnerabilities and risks that might impact the confidentiality, integrity, and availability of information assets. By conducting a thorough assessment, organizations can identify weaknesses, implement appropriate controls, and ensure the overall security of their systems. Therefore, option B, to identify and mitigate security vulnerabilities and risks, is the most accurate description of the purpose of an information security assessment.

47. Which of the following is NOT an essential security principle?

A. Complexity

B. Confidentiality

C. Availability

D. Integrity

Answer: A

Explanation:

Complexity is not considered an essential security principle. The essential security principles are confidentiality, availability, and integrity. Confidentiality ensures that information is only accessible to authorized individuals or entities. It focuses on protecting sensitive data from unauthorized disclosure or access. Availability ensures that information and resources are accessible when needed. It emphasizes the need for systems and networks to be operational and usable, with minimal downtime or interruptions. Integrity ensures that information is accurate, complete, and unaltered. It focuses on maintaining the trustworthiness and reliability of data and preventing unauthorized modifications. Complexity, although important in certain areas of cybersecurity, is not considered an essential security principle on its own. It often relates to the design and implementation of security controls or measures, rather than being a fundamental principle.