CertQuestionsBank

IT Certification Practice Questions

This PDF contains a set of carefully selected practice questions for the 100-160 exam. These questions are designed to reflect the structure, difficulty, and topics covered in the actual exam, helping you reinforce your understanding and identify areas for improvement.

What's Inside:

1. **Topic-focused questions based on the latest exam objectives**
2. **Accurate answer keys to support self-review**
3. **Designed to simulate the real test environment**
4. **Ideal for final review or daily practice**

Important Note:

For full access to the complete question bank and topic-wise explanations, visit:
CertQuestionsBank.com

Our YouTube: https://www.youtube.com/@CertQuestionsBank

FB page: https://www.facebook.com/certquestionsbank

Share some 100-160 exam online questions below.

1.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.

2.What is the purpose of Common Vulnerabilities and Exposures (CVEs)?
A. To protect sensitive information from unauthorized access.
B. To evaluate the effectiveness of cybersecurity measures.
C. To identify hackers and cybercriminals.
D. To categorize and provide unique identifiers for known vulnerabilities.
Answer: D
Explanation:
Common Vulnerabilities and Exposures (CVEs) are used to identify and classify known vulnerabilities in software systems, hardware devices, or networks. Each CVE identifier provides a unique reference point for discussing and addressing specific security weaknesses. By using CVEs, organizations can effectively communicate about vulnerabilities and track their status, enabling better patching and mitigation strategies.

3.Which of the following is an example of a preventive control in computer operations?
A. Backup and recovery procedures
B. Firewall implementation
C. Incident response planning
D. Penetration testing
Answer: B
Explanation:
A firewall is a preventive control in computer operations that helps to protect the network by filtering incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between an internal network and external networks, such as the internet, to prevent unauthorized access and potential attacks.

4.Which of the following best describes the relationship between a business continuity plan (BCP) and a disaster recovery plan (DRP)?
A. A BCP and a DRP are two different terms for the same plan
B. A BCP focuses on maintaining essential functions during a disaster, while a DRP focuses on data backup and restoration
C. A BCP focuses on data backup and restoration, while a DRP focuses on maintaining essential functions during a disaster
D. A BCP and a DRP are separate and unrelated plans within the realm of cybersecurity

Answer: B
Explanation:
While both business continuity plans (BCPs) and disaster recovery plans (DRPs) are essential components of a comprehensive cybersecurity strategy, they have distinct focuses. A BCP primarily deals with the maintenance of essential functions during a disaster, ensuring business continuity, while a DRP primarily deals with data backup, restoration, and recovery processes. Both plans work in tandem to ensure effective cybersecurity practices during a disaster scenario.

5.Why is monitoring security events "as they occur" important in the field of cybersecurity?
A. It allows for rapid detection and response to security incidents.
B. It helps in assessing the effectiveness of security controls.
C. It ensures compliance with industry standards and regulations.
D. It prevents all potential security incidents from occurring.
Answer: A
Explanation:
Monitoring security events "as they occur" is crucial in cybersecurity because it enables rapid detection and response to security incidents. By continuously monitoring and analyzing security events, organizations can identify and respond to incidents promptly, reducing the impact and minimizing potential damage. This proactive approach helps in minimizing downtime, data breaches, and other security risks.

6.Which of the following techniques is commonly used for monitoring security events "as they occur"?
A. Access control lists (ACL)
B. Vulnerability scanning
C. Firewall configuration
D. Intrusion detection systems (IDS)
Answer: D
Explanation:
Intrusion detection systems (IDS) are commonly used for monitoring security events in real-time. IDS monitors network traffic and system activity, looking for signs of unauthorized access, malicious activities, or anomalous behavior. When an intrusion is detected, the system generates alerts for immediate action and response.

7.Which of the following is NOT a component of an incident response policy?
A. Escalation procedures
B. Incident handling procedures
C. Roles and responsibilities
D. Backup and recovery processes
Answer: D
Explanation:
Backup and recovery processes are typically part of an organization's data backup and disaster recovery plan, which is separate from the incident response policy. The incident response policy focuses on defining roles, responsibilities, escalation procedures, and incident handling procedures for responding to cybersecurity incidents.

8.Which of the following best describes social engineering?
A. A method of manipulating individuals to disclose sensitive information
B. A type of malware attack

C. A physical security control
D. A network security protocol
Answer: A
Explanation:
Social engineering refers to the practice of manipulating and deceiving individuals into revealing sensitive information or performing certain actions that may compromise security. It involves exploiting human psychology and trust to gain unauthorized access to systems or obtain confidential information. Social engineering tactics can include phishing emails, impersonation, pretexting, or other forms of manipulation to trick individuals into divulging passwords, account numbers, or other confidential data.

9.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.

10.What is a denial of service (DoS) attack?
A. A technique used by attackers to obtain sensitive information through deception.
B. A software program that is designed to damage, disrupt, or gain unauthorized access to a computer
system.
C. A form of cyber attack that attempts to gain unauthorized access to a network.
D. An attack that overwhelms a target system with a flood of traffic or requests, rendering it inaccessible to legitimate users.
Answer: D
Explanation:
A denial of service (DoS) attack is a type of cyber attack that aims to make a target system or network unavailable to its intended users by overwhelming it with a flood of traffic or requests. This effectively denies legitimate users access to the system.

11.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.

12.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.

13.Which of the following is a best practice for managing security policies and procedures?
A. Implementing a regular review process for security policies
B. Relying solely on default security settings
C. Allowing users to create and manage their own security policies
D. Not documenting the security policies and procedures
Answer: A
Explanation:
Option 1: Correct: Implementing a regular review process for security policies ensures that they are up-to-date and aligned with the organization's current security needs.
Option 2: Incorrect: Relying solely on default security settings is not a best practice as default settings may not provide adequate protection and may not be appropriate for the organization's specific needs.
Option 3: Incorrect: Allowing users to create and manage their own security policies can lead to inconsistencies, lack of control, and potential security vulnerabilities.
Option 4: Incorrect: Not documenting the security policies and procedures makes it difficult to enforce and communicate these policies to employees.

14.Which level of risk category would be associated with a vulnerability that has the potential to cause minor financial loss or impact?
A. High risk
B. Low risk
C. Extremely high risk
D. Medium risk
Answer: B
Explanation:
A vulnerability that has the potential to cause minor financial loss or impact would be categorized as a low-risk level. Low-risk vulnerabilities pose a relatively smaller threat to an organization's assets, systems, or data. While they should not be ignored, low-risk vulnerabilities typically require less immediate attention and resources to mitigate.

15.Which of the following best describes the concept of "defense in depth" in cybersecurity?
A. Establishing strong password policies and enforcing multi-factor authentication
B. Utilizing multiple layers of security measures to protect against threats
C. Deploying advanced encryption algorithms to secure sensitive data
D. Regularly conducting training programs for employees to promote cybersecurity awareness
Answer: B
Explanation:

Defense in depth refers to the practice of implementing multiple layers of security controls and measures to protect against various cyber threats. This approach reduces the likelihood of a single point of failure and increases the overall resilience of the cybersecurity infrastructure.

16.Which of the following is a key requirement for conducting a security compliance audit?
A. A comprehensive understanding of security compliance standards and regulations
B. A certified auditor with expertise in security compliance
C. Compliance monitoring tools and systems
D. A detailed audit plan and checklist
Answer: A
Explanation:
Option 1: Correct. A certified auditor with expertise in security compliance is a key requirement for conducting a security compliance audit. The auditor should have a deep understanding of security compliance standards and regulations to ensure that the audit is performed effectively.
Option 2: Incorrect.
While having a comprehensive understanding of security compliance standards and regulations is important, it is not a key requirement for conducting a security compliance audit. The main requirement is a certified auditor with expertise in security compliance.
Option 3: Incorrect.
Compliance monitoring tools and systems can be helpful during a security compliance audit, but they are not a key requirement. The main requirement is a certified auditor with expertise in security compliance.
Option 4: Incorrect. While having a detailed audit plan and checklist is important, it is not a key requirement for conducting a security compliance audit. The main requirement is a certified auditor with expertise in security compliance.

17.Which regulation is aimed at protecting the privacy and security of personally identifiable information (PII) within the European Union?
A. HIPAA
B. PCI DSS
C. GDPR
D. BYOD
Answer: C
Explanation:
The General Data Protection Regulation (GDPR) is a regulation that aims to protect the privacy and security of personally identifiable information (PII) of individuals within the European Union (EU). It provides guidelines and requirements for data processing, consent, transparency, and breach notification, among other aspects.

18.Which command-line tool is used to query DNS records and obtain information about domain names?
A. traceroute
B. nslookup
C. tcpdump
D. netstat
Answer: B
Explanation:
The correct command-line tool for querying DNS records and obtaining information about domain names is nslookup. It can be used to check the security assessment information related to DNS

configurations, verify the correct mapping of domain names to IP addresses, and troubleshoot any DNS-related issues.

19.Which of the following is a key advantage of multifactor authentication?
A. It allows for anonymous access to systems and resources.
B. It simplifies the authentication process.
C. It eliminates the need for strong passwords.
D. It provides enhanced security by requiring multiple proofs of identity.
Answer: D
Explanation:
Multifactor authentication enhances security by requiring users to present multiple proofs of identity. By combining different factors, such as something you know, something you have, or something you are, it becomes more difficult for unauthorized individuals to gain access. This approach adds an extra layer of protection compared to relying solely on a username and password combination.

20.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.

21.Which command-line tool is commonly used to display active network connections?
A. ping
B. tcpdump
C. netstat
D. nslookup
Answer: C
Explanation:
The correct command-line tool to display active network connections is netstat. It allows you to view open ports, established connections, and other network statistics. It helps in verifying the security assessment information related to active connections.

22.Which of the following is a hardware or software-based network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on predefined security rules?
A. NAC
B. Firewall
C. VPN
D. ACL
Answer: B
Explanation:
A firewall is a hardware or software-based network security device that acts as a barrier between

internal and external networks. It monitors network traffic and applies predefined rules to determine whether to allow or block specific traffic. Firewalls are commonly used to protect network infrastructure and prevent unauthorized access by filtering out potentially harmful or suspicious traffic.

23.Which of the following describes the purpose of a VPN (Virtual Private Network)?
A. To improve network performance and reduce latency
B. To segment a network into multiple smaller networks
C. To provide secure remote access to a private network over the internet
D. To control and filter network traffic based on predefined policies
Answer: C
Explanation:
A VPN (Virtual Private Network) is a technology that enables secure and encrypted communication over a public network, such as the internet. It allows users to establish a secure connection to a private network from remote locations. By encrypting the communication, a VPN ensures confidentiality and integrity of the data transmitted between the remote user and the private network, making it a suitable solution for secure remote access.

24.What is an insider threat?
A. A threat posed by an individual with authorized access to an organization's systems and data.
B. A vulnerability in an organization's network infrastructure.
C. The accidental disclosure of sensitive information.
D. A security breach caused by an external attacker.
Answer: A
Explanation:
Insider threats refer to risks and vulnerabilities that arise from individuals who have authorized access to an organization's systems, networks, or data. These individuals may intentionally or unintentionally cause harm, such as stealing confidential information, sabotaging systems, or disclosing sensitive data to unauthorized entities.

25.Which of the following involves dividing a network into smaller, more manageable segments?
A. DHCP configuration
B. IP addressing
C. VLAN configuration
D. Subnetting
Answer: D
Explanation:
Subnetting is the process of dividing a network into smaller subnetworks, called subnets or subnetworks. It helps in improving network performance, optimizing address allocation, and enhancing network security. Subnetting is typically done by using a subnet mask to determine the network and host portions of an IP address.

26.What is the most effective method to identify and remove unknown malware?
A. Disconnecting the infected system from the network
B. Reinstalling the operating system
C. Scanning the system with multiple antivirus programs
D. Analyzing the behavior of the suspicious program
Answer: D
Explanation:

When dealing with unknown malware, analyzing the behavior of the suspicious program can help to identify any abnormal or malicious activities. This can be done by using behavioral analysis tools, sandboxing, or observing the program's interactions with the system.

27.What is the purpose of Tactics in the context of cybersecurity?
A. To track the impact of a cyberattack on the integrity of data
B. To identify specific cyber threat actors
C. To categorize the methods and strategies employed by cyber threat actors
D. To determine the motive behind a cyberattack
Answer: C
Explanation:
Tactics in cybersecurity refer to the methods and strategies used by cyber threat actors to achieve their objectives. Understanding and categorizing these tactics help organizations assess their vulnerability to specific attacks and develop appropriate defense measures.

28.During the incident handling process, what is the main purpose of conducting a post-incident analysis?
A. Assessing the overall effectiveness of the incident response plan
B. Providing management with a summary of the incident
C. Restoring all affected systems to their pre-incident state
D. Identifying the individuals responsible for the incident
Answer: A
Explanation:
Conducting a post-incident analysis serves the purpose of assessing the overall effectiveness of the incident response plan. It helps identify any weaknesses or areas for improvement in the plan. While identifying responsible individuals, restoring affected systems, and providing management summaries are important aspects, the primary focus of a post-incident analysis is to evaluate and enhance future incident response efforts.

29.During a vulnerability assessment, what is the purpose of making recommendations?
A. To justify the need for additional cybersecurity resources.
B. To allocate responsibility for fixing the vulnerabilities.
C. To mitigate identified vulnerabilities.
D. To obtain management approval for security measures.
Answer: C
Explanation:
The purpose of making recommendations during a vulnerability assessment is to provide guidance on how to mitigate or fix the identified vulnerabilities. These recommendations may include suggested actions, such as applying patches, updating configurations, or implementing additional security controls.

30.Which of the following best describes asset management in the context of cybersecurity?
A. Identifying and protecting valuable resources
B. Monitoring user activity
C. Tracking software licenses

D. Managing network infrastructure
Answer: A
Explanation:
Asset management in a cybersecurity context involves identifying and protecting valuable resources within an organization. This includes identifying critical systems, data, and information that need to be protected from unauthorized access, modification, or destruction.

31.Which of the following is a common authentication protocol used in wireless networks?
A. FTP
B. WPA
C. SSH
D. SMTP
Answer: B
Explanation:
WPA (Wi-Fi Protected Access) is a widely used authentication protocol for securing wireless networks. It provides stronger security than the older WEP (Wired Equivalent Privacy) protocol by utilizing encryption algorithms and dynamic key generation. WPA offers better protection against unauthorized access and helps ensure the confidentiality and integrity of wireless communications.

32.Which command-line tool is commonly used to test network connectivity and measure response time?
A. netstat
B. nslookup
C. tcpdump
D. ping
Answer: D
Explanation:
The correct command-line tool for testing network connectivity and measuring response time is ping. It sends ICMP echo request packets to a specified network device or IP address and waits for the corresponding echo reply, helping to verify if a host is reachable and measure packet latency. However, it is important to note that although ping can provide some basic network testing, it does not capture traffic or packet contents like tcpdump.

33.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.

34.Which technology allows on-demand access to shared pools of configurable computing resources over a network?

A. Virtualization
B. Cloud
C. Proxy
D. DMZ
Answer: B
Explanation:
Cloud computing refers to the delivery of on-demand computing resources, including servers, storage, databases, networking, software, and analytics, over the internet. It provides organizations with the ability to access and use shared pools of configurable computing resources quickly and easily, without the need for extensive upfront infrastructure investments. Cloud computing offers scalability, cost-efficiency, and flexibility, making it an essential component of modern IT environments.

35.When should a firewall rule triggering block external access to a network resource be escalated?
A. Only if the access was authorized.
B. Always, regardless of authorization.
C. Only if the access attempt is from a known malicious IP address.
D. Never, as it is a normal security function of a firewall.
Answer: D
Explanation:
Blocking external access to a network resource is a normal security function of a firewall and does not necessarily require escalation. Firewalls are designed to monitor and control incoming and outgoing network traffic based on predetermined rules and configurations. However, if the rule is triggered unexpectedly or causes disruption to critical services, it may be appropriate to escalate the issue for further investigation or adjustment of the firewall rule.

36.Which threat intelligence technique involves utilizing known patterns or characteristics of threats to identify and block them?
A. Reputation-based Detection
B. Anomaly-based Detection
C. Indicators of Compromise (IoCs)
D. Signature-based Detection
Answer: D
Explanation:
Signature-based detection relies on identifying known patterns, signatures, or characteristics of threats.
It uses these signatures to detect and block potential threats in network traffic.

37.What is the role of policies in vulnerability assessment?
A. They determine the frequency of vulnerability assessments.
B. They specify the criteria for prioritizing vulnerabilities.
C. They define the rules and guidelines for vulnerability scanning.
D. They outline the consequences of not fixing vulnerabilities.
Answer: C
Explanation:
Policies play a crucial role in vulnerability assessment by defining the rules and guidelines for conducting vulnerability scanning activities. These policies ensure consistency and provide direction on how to
approach vulnerability assessments, including the scope, methodology, and frequency of the

assessments.

38.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.

39.What is a common outcome of the policy development phase in cybersecurity planning?
A. Implementation of technical controls
B. Creation of incident response plans
C. Identification of security vulnerabilities
D. Development of security awareness training programs
Answer: D
Explanation:
The policy development phase in cybersecurity planning involves creating and documenting the policies and procedures that guide the organization's cybersecurity practices. It often includes the development of security awareness training programs to educate employees about their roles and responsibilities in maintaining cybersecurity and to promote good security practices throughout the organization.

40.What is one of the main objectives of documenting cybersecurity incidents?
A. To create a historical record of incidents for legal purposes
B. To assign blame to individuals responsible for the incident
C. To minimize the impact of cyber attacks
D. To divert attention from the incident
Answer: C
Explanation:
Documenting cybersecurity incidents helps organizations understand the nature, extent, and impact of the incident. By documenting incidents, organizations can analyze trends, develop strategies to prevent future incidents, and minimize the impact of cyber attacks.

41.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.

42.What is the main purpose of a disaster recovery plan?
A. Recovering data after a disaster
B. Preventing disasters from occurring
C. Minimizing the impact of disasters
D. Identifying potential threats and vulnerabilities
Answer: A
Explanation:
The primary purpose of a disaster recovery plan is to ensure that data, systems, and operations can be restored in a timely manner following a disaster. It focuses on recovering critical resources and minimizing downtime to resume normal business operations as quickly as possible.

43.Which of the following is a benefit of utilizing automated threat intelligence within a cybersecurity system?
A. Increased vulnerability detection
B. All of the above
C. Improved incident response time
D. Reduced false positives
Answer: B
Explanation:
Automated threat intelligence systems gather and analyze vast amounts of data to identify potential threats and vulnerabilities. By utilizing these systems, organizations can benefit from reduced false positives, increased vulnerability detection, and improved incident response time. This comprehensive approach enhances the overall effectiveness of a cybersecurity system.

44.Which endpoint security mechanism is used to secure data transmitted between the endpoint and the
network?
A. Firewall
B. Antivirus
C. Encryption
D. Intrusion Detection System (IDS)
Answer: C
Explanation:
Encryption is the mechanism used to secure data transmitted between the endpoint and the network. By encrypting the data, it becomes unreadable to unauthorized parties, ensuring the confidentiality and integrity of the information being transmitted. Encryption transforms the data into a ciphertext, which can only be decrypted back into its original form using the proper encryption key. This helps protect sensitive and confidential data from interception and unauthorized access during transmission over the network.

45.What is the purpose of a Virtual Private Network (VPN) in cybersecurity?
A. To monitor network traffic for potential security threats
B. To encrypt traffic between two networks
C. To filter network traffic based on predefined rules
D. To authenticate users before granting them access

Answer: B
Explanation:
A Virtual Private Network (VPN) is a secure connection established over a public network, such as the internet. Its primary purpose is to encrypt traffic between two networks or between an individual user and a network. By using encryption protocols, VPNs ensure that data transmitted over the network remains confidential and secure, protecting it from unauthorized access or interception.

46.What action should be taken when a user reports a suspicious email with a potential phishing link?
A. Click on the link to verify its validity before taking any action.
B. Forward the email to other users to raise awareness about potential threats.
C. Escalate the issue to the security team for further investigation.
D. Delete the email and inform the user that it is safe to proceed.
Answer: C
Explanation:
When a user reports a suspicious email with a potential phishing link, it is important to escalate the issue to the security team for further investigation. Phishing attacks can pose significant risks to organizations, and it is crucial to involve the appropriate experts to assess and address the threat appropriately.

47.What does hardening mean in the context of cybersecurity?
A. Removing all vulnerabilities from a system or network
B. Implementing cybersecurity policies and regulations
C. Creating a backup of critical data and configurations
D. Making a system more resistant to threats and attacks
Answer: D
Explanation:
Hardening refers to the process of securing a system by reducing its vulnerability to potential threats and attacks. It involves implementing security best practices, such as disabling unnecessary services, applying patches and updates, configuring access controls, strengthening passwords, and employing additional security measures like firewalls or intrusion detection systems. Hardening helps ensure systems are less susceptible to exploitation.