Free Cisco 100-160 CCST Cybersecurity Practice Questions

Shared by Hanson on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are collecting data after a suspected intrusion on the local LAN.

You need to capture incoming IP packets to a file for an investigator to analyze.

Which two tools should you use? (Choose 2.)

Options:

A- Wireshark
B- tcpdump
C- Nmap
D- netstat

Answer:

A, B

Explanation:

The CCST Cybersecurity Study Guide specifies that both Wireshark and tcpdump are packet capture tools that can record network traffic to a file for later analysis.

'Wireshark provides a graphical interface for packet capture and analysis. Tcpdump is a command-line tool that captures packets for detailed offline review.'

(CCST Cybersecurity, Incident Handling, Network Traffic Analysis section, Cisco Networking Academy)

A is correct: Wireshark is widely used for packet capture and analysis.

B is correct: tcpdump is a CLI-based packet capture tool.

C (Nmap) is for network scanning, not packet capture.

D (netstat) displays network connections and ports but does not capture packets.

Question 2

Question Type: MultipleChoice

What is the primary purpose of running a vulnerability scan on your network?

Options:

A- To identify and document the locations of customer and financial databases
B- To automatically prioritize security weaknesses for immediate remediation
C- To determine whether systems are subject to CVEs that could be exploited by adversaries
D- To correlate event logs on multiple servers in order to generate intrusion alerts

Answer:

C

Explanation:

The CCST Cybersecurity Study Guide states that vulnerability scanning is an automated process used to identify known security weaknesses in systems, software, and network devices. These scans compare system configurations and software versions against databases of known vulnerabilities, such as the Common Vulnerabilities and Exposures (CVE) list.

'A vulnerability scan is an automated test that checks systems and networks for known weaknesses by matching them against a database of vulnerabilities such as CVEs. This allows administrators to identify exploitable conditions before they are leveraged by attackers.'

(CCST Cybersecurity, Vulnerability Assessment and Risk Management, Vulnerability Scanning section, Cisco Networking Academy)

A is asset discovery, not vulnerability scanning.

B may be part of remediation planning but is not the primary purpose.

C is correct: Scans detect if systems have vulnerabilities associated with CVEs.

D describes SIEM (Security Information and Event Management) log correlation, not vulnerability scanning.

Question 3

Question Type: MultipleChoice

You are going to perform a penetration test on a company LAN. As part of your preparation, you access the company's websites, view webpage source code, and run internet searches to

uncover domain information. You also use social media to gather details about the company and its employees.

Which type of reconnaissance activities are you performing?

Options:

A- Passive
B- Active
C- Offline
D- Invasive

Answer:

A

Explanation:

The CCST Cybersecurity Study Guide explains that reconnaissance is the process of collecting information about a target before attempting exploitation.

'Passive reconnaissance is conducted without directly engaging with the target systems. Examples include reviewing public websites, examining HTML source code, querying public DNS records, and using social media to gather information. Since no packets are sent directly to the target system, it reduces the risk of detection.'

(CCST Cybersecurity, Vulnerability Assessment and Risk Management, Reconnaissance Techniques section, Cisco Networking Academy)

Passive (A) is correct because all actions described --- viewing public pages, searching online, and checking social media --- involve no direct interaction that could alert the target.

Active (B) would involve direct probing, like port scans or vulnerability scans.

Offline (C) is not an official reconnaissance classification in this context.

Invasive (D) is a general term and not used as a standard reconnaissance category in CCST material.

Question 4

Question Type: MultipleChoice

An employee accidentally sends an email containing sensitive corporate information to an

external email address.

Which type of threat does this scenario describe?

Options:

A- Logic bomb
B- Malware
C- Phishing
D- Insider

Answer:

D

Explanation:

The CCST Cybersecurity Study Guide explains that an insider threat is any threat to an organization that comes from people within the organization---employees, contractors, or business partners---who have inside information concerning the organization's security practices, data, and systems. Insider threats may be intentional or unintentional.

'An insider threat can be malicious or accidental. Employees may unintentionally cause data breaches by mishandling sensitive information, such as sending it to the wrong recipient.'

(CCST Cybersecurity, Essential Security Principles, Threat Actor Types section, Cisco Networking Academy)

A (Logic bomb) is malicious code triggered by conditions.

B (Malware) is malicious software, unrelated to accidental email leaks.

C (Phishing) is an external social engineering attack.

D is correct: This is an unintentional insider threat.

Question 5

Question Type: MultipleChoice

Which security measure can prevent unauthorized devices from automatically connecting to a corporate network through unused switch ports?

Options:

A- Port security
B- VLAN trunking
C- NAT
D- VPN

Answer:

A

Explanation:

The CCST Cybersecurity Study Guide explains that port security on switches can be configured to limit the number of MAC addresses allowed on a port, or to restrict it to specific devices.

'Port security can prevent unauthorized access by limiting or specifying the MAC addresses allowed to connect through a given switch port. This mitigates risks from rogue devices connecting to the network.'

(CCST Cybersecurity, Basic Network Security Concepts, Switch Security section, Cisco Networking Academy)

Question 6

Question Type: MultipleChoice

How does sandboxing help with the analysis of malware?

Options:

A- It defines the suspicious or malicious applications that should be blocked.
B- It specifies the applications that are authorized for use on the network.
C- It allows suspicious applications to run in a safe and isolated testing environment.
D- It restricts traffic from passing from one network to another.

Answer:

C

Explanation:

The CCST Cybersecurity Study Guide explains that sandboxing is a security technique that executes suspicious programs in a controlled and isolated environment, preventing them from affecting production systems while enabling behavior analysis.

'Sandboxing isolates a suspected application in a secure, controlled environment where it can be executed and analyzed without risking damage to the host system or network.'

(CCST Cybersecurity, Endpoint Security Concepts, Malware Analysis Techniques section, Cisco Networking Academy)

Question 7

Question Type: MultipleChoice

Which step should be performed immediately after identifying a critical vulnerability affecting internet-facing systems?

Options:

A- Document the vulnerability in the annual security report.
B- Apply the vendor patch or mitigation.
C- Schedule a quarterly penetration test.
D- Change the default administrator passwords.

Answer:

B

Explanation:

The CCST Cybersecurity Study Guide states that after confirming a vulnerability is relevant and critical, the next step is to apply available patches or mitigations as soon as possible to reduce the attack surface.

'When a critical vulnerability is identified, remediation steps such as applying patches or configuration changes should be implemented immediately to prevent exploitation.'

(CCST Cybersecurity, Vulnerability Assessment and Risk Management, Vulnerability Remediation section, Cisco Networking Academy)

Question 8

Question Type: MultipleChoice

A restaurant installs a second wireless router that only employees can use.

Which statement describes how to securely configure the new router?

Options:

A- Configure the new router to filter IP addresses.
B- Configure the SSID with broadcast disabled.
C- Configure a higher signal strength to allow coverage in the parking lot.
D- Configure the SSID with the same SSID used by the customer router.

Answer:

B

Explanation:

The CCST Cybersecurity Study Guide explains that disabling SSID broadcast hides the network from casual scanning, adding a layer of obscurity. While not a complete security measure, when combined with WPA2/WPA3 encryption and strong passwords, it can help protect private wireless networks, especially in environments with separate employee and guest access.

'Disabling SSID broadcast can reduce the visibility of a wireless network, making it less likely to be detected by casual attackers. This should be combined with strong encryption and authentication.'

(CCST Cybersecurity, Basic Network Security Concepts, Wireless Security section, Cisco Networking Academy)

A (IP filtering) provides limited protection and is harder to manage for employee devices.

B is correct: Disabling SSID broadcast adds an extra layer of obscurity for the employee network.

C would make the network easier to access from outside the premises, which is less secure.

D would cause network conflicts and make segmentation impossible.

Question 9

Question Type: MultipleChoice

You work for a hospital that stores electronic protected health information (ePHI) in an online portal. Authorized employees can use their mobile devices to access patient ePHI.

You need to ensure that employees' mobile devices comply with HIPAA regulations.

Which safeguard should you develop and implement?

Options:

A- An ownership policy for employees' mobile devices
B- A contingency plan
C- A policy that requires multi-factor authentication to use the mobile device
D- A policy to govern how ePHI is removed from mobile devices

Answer:

D

Explanation:

The CCST Cybersecurity Study Guide notes that HIPAA (Health Insurance Portability and Accountability Act) requires that ePHI be protected both in storage and when devices are decommissioned or repurposed. This includes implementing data removal policies for mobile devices.

'HIPAA requires procedures for the removal of electronic protected health information (ePHI) from devices before disposal, reuse, or reassignment.'

(CCST Cybersecurity, Essential Security Principles, Regulatory Compliance section, Cisco Networking Academy)

Question 10

Question Type: MultipleChoice

What is the primary purpose of running a vulnerability scan on your network?

Options:

A- To identify and document the locations of customer and financial databases
B- To automatically prioritize security weaknesses for immediate remediation
C- To determine whether systems are subject to CVEs that could be exploited by adversaries
D- To correlate event logs on multiple servers in order to generate intrusion alerts

Answer:

C

Explanation:

The CCST Cybersecurity Study Guide states that vulnerability scanning is an automated process used to identify known security weaknesses in systems, software, and network devices. These scans compare system configurations and software versions against databases of known vulnerabilities, such as the Common Vulnerabilities and Exposures (CVE) list.

'A vulnerability scan is an automated test that checks systems and networks for known weaknesses by matching them against a database of vulnerabilities such as CVEs. This allows administrators to identify exploitable conditions before they are leveraged by attackers.'

(CCST Cybersecurity, Vulnerability Assessment and Risk Management, Vulnerability Scanning section, Cisco Networking Academy)

A is asset discovery, not vulnerability scanning.

B may be part of remediation planning but is not the primary purpose.

C is correct: Scans detect if systems have vulnerabilities associated with CVEs.

D describes SIEM (Security Information and Event Management) log correlation, not vulnerability scanning.

Question 11

Question Type: MultipleChoice

You are going to perform a penetration test on a company LAN. As part of your preparation, you access the company's websites, view webpage source code, and run internet searches to uncover domain information. You also use social media to gather details about the company and its employees.

Which type of reconnaissance activities are you performing?

Options:

A- Passive
B- Active
C- Offline
D- Invasive

Answer:

A

Explanation:

The CCST Cybersecurity Study Guide explains that reconnaissance is the process of collecting information about a target before attempting exploitation.

'Passive reconnaissance is conducted without directly engaging with the target systems. Examples include reviewing public websites, examining HTML source code, querying public DNS records, and using social media to gather information. Since no packets are sent directly to the target system, it reduces the risk of detection.'

(CCST Cybersecurity, Vulnerability Assessment and Risk Management, Reconnaissance Techniques section, Cisco Networking Academy)

Passive (A) is correct because all actions described --- viewing public pages, searching online, and checking social media --- involve no direct interaction that could alert the target.

Active (B) would involve direct probing, like port scans or vulnerability scans.

Offline (C) is not an official reconnaissance classification in this context.

Invasive (D) is a general term and not used as a standard reconnaissance category in CCST material.