ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Cisco

Code: 100-160

Exam: Cisco Certified Support Technician (CCST) Cybersecurity (CCST Cybersecurity)

https://www.examsnest.com/exam/100-160/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.0

Question: 1

How does a honeypot enhance network security?

A. It monitors network traffic and sends alerts when potential threats are detected.
B. It acts as a decoy and diverts malicious traffic away from important systems.
C. It isolates external-facing services from the Internet and protects them from attack.
D. It detects and prevents identified threats through real-time packet inspection.

Answer: B

Explanation:

According to the Cisco Certified Support Technician (CCST) Cybersecurity Study Guide, a honeypot is a security mechanism that appears to be a legitimate system or resource but is intentionally made vulnerable to attract attackers. Its purpose is not to serve legitimate users but to detect, study, and sometimes divert malicious activity.
"A honeypot is a decoy system or service designed to attract and engage attackers. By simulating a target of interest, it allows security teams to monitor attack methods, collect intelligence, and sometimes divert threats away from production systems. Honeypots do not prevent attacks but help in identifying them and understanding adversary tactics."
(CCST Cybersecurity, Basic Network Security Concepts, Honeypots and Honey Nets section, Cisco Networking Academy)
In this context:
Option A describes an IDS (Intrusion Detection System), not a honeypot.
Option C refers to a DMZ (Demilitarized Zone), not a honeypot.
Option D describes an IPS (Intrusion Prevention System).
Option B correctly identifies a honeypot's role as a decoy to divert or engage attackers.

Question: 2

Which data type is protected through hard disk encryption?

A. Data in process
B. Data in transit
C. Data in use
D. Data at rest

Answer: D

Explanation:

The CCST Cybersecurity Study Guide explains that hard disk encryption is a method used to protect data stored on a physical device from unauthorized access.
"Data at rest refers to data stored on a device, such as files on a hard drive, SSD, or removable media. Hard disk encryption protects data at rest by converting it into an unreadable format unless accessed with the correct decryption key."
(CCST Cybersecurity, Essential Security Principles, Data States and Protection Methods section, Cisco Networking Academy)
Data in process refers to data actively being handled by applications in memory (RAM), which is not the primary target of disk encryption.
Data in transit is protected via encryption methods such as TLS, not disk encryption.
Data in use is accessed and manipulated by programs in real-time, also not the primary scope of disk encryption.
Data at rest is the correct answer, as hard disk encryption directly safeguards stored files.

Question: 3

Your supervisor suspects that someone is attempting to gain access to a Windows computer by guessing user account IDs and passwords. The supervisor asks you to use the Windows Event Viewer security logs to verify the attempts.
Which two audit policy events provide information to determine whether someone is using invalid credentials to attempt to log in to the computer? (Choose 2.)
Note: You will receive partial credit for each correct selection.

A. Object access failure
B. Account logon failure
C. Account lockout success
D. Account logoff success

Answer: BC

Explanation:

According to the CCST Cybersecurity course, Windows Event Viewer's Security logs record authentication-related events that can help identify password-guessing attempts (also known as brute force attacks).
"The Account logon failure event indicates that an authentication attempt has failed, which may suggest incorrect credentials were used. Multiple such events in a short time frame can indicate a brute-force attack. The Account lockout success event confirms that an account has been locked due to repeated failed logon attempts, which further supports the suspicion of password-guessing attacks."
(CCST Cybersecurity, Incident Handling, Monitoring and Analyzing Security Events section, Cisco Networking Academy)
Object access failure relates to unauthorized attempts to open or modify files, not login attempts

Account logon failure (B) shows failed login attempts due to invalid credentials.
Account lockout success (C) confirms that repeated login failures have triggered a lockout.
Account logoff success is a normal event and does not indicate malicious activity.

Question: 4

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?

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: 5

Your manager asks you to review the output of some vulnerability scans and report anything that may require escalation.
Which two findings should you report for further investigation as potential security vulnerabilities? (Choose 2.)

A. Encrypted passwords
B. Disabled firewalls
C. Open ports
D. SSH packets

Answer: BC

Explanation:

The CCST Cybersecurity course teaches that vulnerability scan results should be reviewed for misconfigurations and exposures that can be exploited by attackers.
"Disabled firewalls expose systems to direct network attacks and should be treated as critical findings. Open ports can indicate unnecessary or unsecured services running, which may provide entry points for attackers. These findings should be escalated for remediation or further security hardening."
(CCST Cybersecurity, Vulnerability Assessment and Risk Management, Analyzing and Responding to Scan Results section, Cisco Networking Academy)
Encrypted passwords (A) are good practice, not a vulnerability.
Disabled firewalls (B) leave systems defenseless against incoming attacks.
Open ports (C) can be exploited if the services they expose are vulnerable or misconfigured.
SSH packets (D) are normal in secure remote administration and are not inherently a vulnerability.

Thank You for trying the PDF Demo

Vendor: Cisco

Code: 100-160

Exam: Cisco Certified Support Technician (CCST) Cybersecurity (CCST Cybersecurity)

https://www.examsnest.com/exam/100-160/