KaozhengPro

# IT認證考試題庫

# 專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

**Exam** : **N10-009**

**Title** : CompTIA Network+ Certification

**Version** : DEMO

1.A client wants to increase overall security after a recent breach.
Which of the following would be best to implement? (Select two.)
A. Least privilege network access
B. Dynamic inventeries
C. Central policy management
D. Zero-touch provisioning
E. Configuration drift prevention
F. Subnet range limits
**Answer:** A,C
**Explanation:**
To increase overall security after a recent breach, implementing least privilege network access and central policy management are effective strategies.
Least Privilege Network Access: This principle ensures that users and devices are granted only the access necessary to perform their functions, minimizing the potential for unauthorized access or breaches. By limiting permissions, the risk of an attacker gaining access to critical parts of the network is reduced.
Central Policy Management: Centralized management of security policies allows for consistent and streamlined implementation of security measures across the entire network. This helps in quickly responding to security incidents, ensuring compliance with security protocols, and reducing the chances of misconfigurations.
Network
Reference: CompTIA Network+ N10-007 Official Certification Guide: Discusses network security principles, including least privilege and policy management.
Cisco Networking Academy: Provides training on implementing security policies and access controls.
Network+ Certification All-in-One Exam Guide: Covers strategies for enhancing network security and managing policies effectively.

2.A network administrator needs to connect two routers in a point-to-point configuration and conserve IP space.
Which of the following subnets should the administrator use?
A. 724
B. /26
C. /28
D. /30
**Answer:** D
**Explanation:**
Using a /30 subnet mask is the most efficient way to conserve IP space for a point-to-point connection between two routers. A /30 subnet provides four IP addresses, two of which can be assigned to the router interfaces, one for the network address, and one for the broadcast address. This makes it ideal for point-to-point links where only two usable IP addresses are needed.
Reference: CompTIA Network+ study materials and subnetting principles.

3.A network administrator determines that some switch ports have more errors present than expected. The administrator traces the cabling associated with these ports.

Which of the following would most likely be causing the errors?
A. arp
B. tracert
C. nmap
D. ipconfig
**Answer:** D

4.A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare.
Which of the following tools would help identify which ports are open on the remote file server?
A. Dig
B. Nmap
C. Tracert
D. nslookup
**Answer:** B
**Explanation:**
Nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a computer network. It can be used to identify which ports are open on a remote server, which can help diagnose access issues to services like a remote file server.
Port Scanning: Nmap can perform comprehensive port scans to determine which ports are open and what services are running on those ports.
Network Discovery: It provides detailed information about the host's operating system, service versions, and network configuration.
Security Audits: Besides troubleshooting, Nmap is also used for security auditing and identifying potential vulnerabilities.
Network
Reference: CompTIA Network+ N10-007 Official Certification Guide: Covers network scanning tools and their uses.
Nmap Documentation: Official documentation provides extensive details on how to use Nmap for port scanning and network diagnostics.
Network+ Certification All-in-One Exam Guide: Discusses various network utilities, including Nmap, and their applications in network troubleshooting.

5.Which of the following allows for the interception of traffic between the source and destination?
A. Self-signed certificate
B. VLAN hopping
C. On-path attack
D. Phishing
**Answer:** C
**Explanation:**
An on-path attack (formerly known as a man-in-the-middle (MITM) attack) involves intercepting and potentially altering communications between two parties without their knowledge. This can be done via techniques like ARP poisoning, rogue access points, or SSL stripping. Breakdown of Options:

A. Self-signed certificate – These are untrusted SSL certificates but do not intercept traffic.
B. VLAN hopping – VLAN hopping exploits VLAN misconfigurations but does not necessarily intercept communications.
C. On-path attack – Correct answer. This intercepts and modifies traffic between two endpoints.
D. Phishing – Phishing tricks users into revealing credentials rather than intercepting network traffic.
Reference: CompTIA Network+ (N10-009) Official Study Guide – Domain 3.2: Explain common security concepts.
NIST SP 800-115: Guide to Security Testing and Assessments