N10-009 Q&As

CompTIA Network+

Pass CompTIA N10-009 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/n10-009.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

Which of the following allows a remote user to connect to the network?

A. Command-line interface

B. API gateway

C. Client-to-site VPN

D. Jump box

Correct Answer: C

A Client-to-Site VPN allows a remote user to securely connect to a company\\'s internal network, providing access as if they were physically on-site.

QUESTION 2

To reduce costs and increase mobility, a Chief Technology Officer (CTO) wants to adopt cloud services for the organization and its affiliates. To reduce the impact for users, the CTO wants key services to run from the on-site data center and enterprise services to run in the cloud. Which of the following deployment models is the best choice for the organization?

A. Public

B. Hybrid

C. SaaS

D. Private

Correct Answer: B

A hybrid cloud deployment model is the best choice for the CTO\\'s requirements. It allows the organization to run key services from the on-site data center while leveraging the cloud for enterprise services. This approach provides flexibility, scalability, and cost savings, while also minimizing disruptions to users by keeping critical services local. The hybrid model integrates both private and public cloud environments, offering the benefits of both.References: CompTIA Network+ study materials and cloud computing principles.

QUESTION 3

Which of the following kinds of targeted attacks uses multiple computers or bots to request the same resource repeatedly?

A. On-path

B. DDoS

C. ARP spoofing

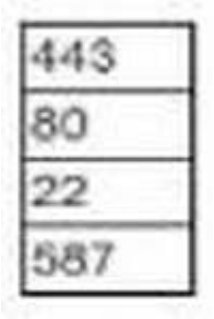
D. MAC flooding

Correct Answer: B

A DDoS makes the most sense because in a DDoS attack, the threat actor uses multiple computers that are infected to constantly make requests to a server which overwhelms it and causes network interruption.

QUESTION 4

A company is hosting a secure that requires all connections to the server to be encrypted. A junior administrator needs to harded the web server. The following ports on the web server. The following ports on the web server are open:



Which of the following ports should be disabled?

A. 22

B. 80

C. 443

D. 587

Correct Answer: B

For a web server that requires all connections to be encrypted, port 80 (HTTP) should be disabled. Port 80 is used for unencrypted web traffic, whereas port 443 is used for HTTPS, which provides encrypted communication. Port 80 (HTTP):

This port is used for unsecured web traffic. Disabling this port ensures that all web traffic must use HTTPS, which encrypts the data in transit. Port 443 (HTTPS): This port is used for secure web traffic via SSL/TLS encryption. Keeping this

port open ensures that secure connections can be made to the web server.

Other Ports:

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Discusses the roles and security implications of various ports and protocols. Cisco Networking Academy: Provides training on secure web server configuration and port management.

Network+ Certification All-in-One uide: Covers port security and best practices for securing web servers.

QUESTION 5

Which of the following network devices converts wireless signals to electronic signals?

A. Router

B. Firewall

C. Access point

D. Load balancer

Correct Answer: C

Role of an Access Point (AP):

uk.co.certification.simulator.questionpool.PList@7be106c3 Functionality:

Comparison with Other Devices:

Deployment:

References:

CompTIA Network+ study materials on wireless networking and access points.

QUESTION 6

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 wold help identify which ports are open on the remote file server?

A. Dig

B. Nmap

C. Tracert

D. nslookup

Correct Answer: B

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 References:

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 uide: Discusses various network utilities, including Nmap, and

their applications in network troubleshooting.

QUESTION 7

Following a fire in a data center, the cabling was replaced. Soon after, an administrator notices network issues. Which of the following are the most likely causes of the network issues? (Select two).

A. The switches are not the correct voltage.

B. The HVAC system was not verified as fully functional after the fire.

C. The VLAN database was not deleted before the equipment was brought back online.

D. The RJ45 cables were replaced with unshielded cables.

E. The wrong transceiver type was used for the new termination.

F. The new RJ45 cables are a higher category than the old ones.

Correct Answer: DE

Unshielded cables (D) are more prone to interference and may not be suitable for certain environments, especially after a fire where interference could be heightened. Using the wrong transceiver (E) for new terminations can lead to compatibility issues, causing network failures.

QUESTION 8

Before using a guest network, an administrator requires users to accept the terms of use

Which of the following is the best way to accomplish this goal?

A. Pre-shared key

B. Autonomous access point

C. Captive portal

D. WPA2 encryption

Correct Answer: C

A captive portal is a web page that users must view and interact with before being granted access to a network. It is commonly used in guest networks to enforce terms of use agreements. When a user connects to the network, they are redirected to this portal where they must accept the terms of use before proceeding. This method ensures that users are aware of and agree to the network\\'s policies, making it the best choice for this scenario. References: CompTIA Network

+ Exam Objectives and official study guides.

QUESTION 9

A network administrator is switching to IPv6 and wants to be able to use packet-tracing software on the network to monitor traffic. The administrator wants to set up the IP addressing to include the MAC address of each machine that is connected. Which of the following should the administrator implement? (Choose two.)

A. EUI-64

B. RFC1819

C. APIPA

D. DHCPv6

E. SLAAC

F. CIDR

Correct Answer: AE

QUESTION 10

Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?

A. To encrypt sensitive data in transit

B. To secure the endpoint

C. To maintain contractual agreements

D. To comply with data retentin requirements

Correct Answer: A

The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user\\'s device and the corporate network, ensuring that data

is encrypted and protected from interception.

Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks. Data Protection: Essential for industries handling sensitive information, such as insurance

brokerages, to protect customer data and comply with regulatory requirements.

Security: Enhances overall network security by providing secure remote access for employees.

Network References:

CompTIA Network+ N10-007 Official Certification Guide: Discusses the role of VPNs in securing data in transit.

Cisco Networking Academy: Provides training on VPN technologies and their importance in data security.

Network+ Certification All-in-One uide: Explains VPN usage and its benefits in protecting sensitive information.

QUESTION 11

Which of the following is a major difference between a router and a Layer 3 switch?

A. A router can perform PAT, but a Layer 3 switch cannot.

B. A Layer 3 switch is more efficient than a router.

C. A router uses higher speed interfaces than a Layer 3 switch.

D. A Layer 3 switch can run more routing protocols than a router.

Correct Answer: B

QUESTION 12

A network administrator notices interference with industrial equipment in the 2.4GHz range. Which of the following technologies would most likely mitigate this issue? (Select two).

A. Mesh network

B. 5GHz frequency

C. Omnidirectional antenna

D. Non-overlapping channel

E. Captive portal

F. Ad hoc network

Correct Answer: B

Understanding 2.4GHz Interference:

uk.co.certification.simulator.questionpool.PList@167c5740 Mitigation Strategies:

Why Other Options are Less Effective:

Implementation:

References:

CompTIA Network+ study materials on wireless networking and interference mitigation.

QUESTION 13

A user is unable to navigate to a website because the provided URL is not resolving to the correct IP address. Other users are able to navigate to the intended website without issue. Which of the following is most likely causing this issue?

A. Hosts file

B. Self-signed certificate

C. Nameserver record

D. IP helper ANS

Correct Answer: A

Role of the Hosts File:

uk.co.certification.simulator.questionpool.PList@5a62cfc0 Common Issues with the Hosts File:

Why Other Options are Less Likely:

Troubleshooting Steps:

References:

CompTIA Network+ study materials and system administration documentation.

QUESTION 14

A network administrator wants to implement an authentication process for temporary access to an organization\\'s network. Which of the following technologies would facilitate this process?

A. Captive portal

B. Enterprise authentication

C. Ad hoc network

D. WPA3

Correct Answer: A

A captive portal is a technology that facilitates the authentication process for temporary access to a network. It is commonly used in public Wi-Fi hotspots, hotels, airports, and other environments where temporary network access is provided. When users connect to the network, they are redirected to a captive portal page where they must authenticate or agree to terms and conditions before gaining access to the internet or other network resources.

QUESTION 15

Which of the following is the correct order of components in a bottom-up approach for the three-tier hierarchical model?

A. Access, distribution, and core

B. Core, root, and distribution

C. Core, spine, and leaf

D. Access, core, and roof

Correct Answer: A

The three-tier hierarchical model in network design consists of three layers: access, distribution, and core. The access layer is where devices like PCs and printers connect to the network. The distribution layer aggregates the data received

from the access layer switches before it is transmitted to the core layer, which is responsible for high-speed data transfer and routing. This approach improves scalability and performance in larger networks.

References: CompTIA Network+ Exam Objectives and official study guides.