Free Questions for N10-008 by dumpshq

Shared by Luna on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A network administrator is adding a new wired IoT device to the internal network. The only devices that will be communicating are the HVAC system and the IoT device. Which of the following should the network administrator do?

Options:

A- Set up a secure VM.

B- Implement a reverse proxy.

C- Set up the guest network isolation.

D- Configure a dedicated VLAN.

Answer:

D

Explanation:

When adding a new wired IoT device that will only communicate with the HVAC system, it is best practice to configure a dedicated VLAN. This isolates the traffic between the IoT device and the HVAC system from the rest of the network, enhancing security and network efficiency.

CompTIA Network+ N10-008 Full Course for Beginners - Configuring SOHO Networks4

Network+ (Plus) Certification | CompTIA IT Certifications

Question 2

Question Type: **MultipleChoice**

Which of the following describes the differences between switches and hubs?

Options:

A- Switches operate on the physical layer, while hubs operate on the data link layer.

B- Switches operate on the session layer, while hubs operate on the transport layer.

C- Switches operate on the data link layer, while hubs operate on the physial layer.

D- Switches operate on the transport layer, while hubs operate on the data link layer.

Answer:

C

Explanation:

Switches operate at the data link layer (Layer 2) of the OSI model and make decisions based on MAC addresses. Hubs, on the other hand, operate at the physical layer (Layer 1) and simply repeat the signals they receive to all connected devices without any filtering or decision-making.

Networking Devices -- N10-008 CompTIA Network+ : 2.1

Question 3

Question Type: MultipleChoice

An organization needs a solution that will inspect network traffic, determine security threats using signature-based rules, and block the traffic in real time based on the security assessment. Which of the following network devices will support these requirements?

Options:

A- SIEM

B- VPN

C- IPS

D- DLP

Answer:

C

Explanation:

An Intrusion Prevention System (IPS) is designed to inspect network traffic, identify malicious activity using signature-based rules, and block potentially harmful traffic in real time. This aligns with the requirements stated in the question.

CompTIA Network+ N10-008 Certification Study Guide1

CompTIA Network+ N10-007 vs.N10-008: What's New

Question 4

Question Type: **MultipleChoice**

Which of the following fields are negotiated during the three-way-handshake process? (Select three).

Options:

A- Sequence number

B- MTU

C- Window size

D- MSS

E- TTL

F- Flags

G- Acknowledgment number

H- CRC

Answer:

A, C, G

Explanation:

During the TCP three-way handshake process, the following fields are negotiated:

A . Sequence number: Initial sequence numbers are established during the handshake to keep track of the segments in the communication.

C . Window size: This determines the amount of data that can be sent before receiving an acknowledgment.

G . Acknowledgment number: This confirms receipt of the data and also indicates the next expected byte.

The other options are not negotiated during the three-way handshake:

B . MTU (Maximum Transmission Unit): This is determined at the network layer and is not negotiated during the handshake.

D . MSS (Maximum Segment Size): This is communicated during the handshake but not negotiated; it's declared by the sender to inform the receiver of the maximum segment size it can handle.

E . TTL (Time To Live): This is set in each IP packet to limit its lifespan and is not negotiated during the handshake.

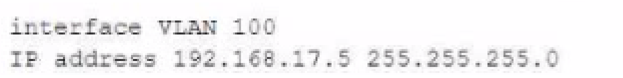
F- Flags: Specific flags are used during the handshake (SYN and ACK), but they are not "negotiated" per se.

H) CRC (Cyclic Redundancy Check): This is used for error-checking in frames at the data link layer and is not part of the three-way handshake.

Question 5

Question Type: MultipleChoice

An engineer recently installed a new distribution switch and connected two servers provisioned with the following IPs: 192.168.17.20 and 192.168.17.30. The servers cannot connect to the Internet, but they can reach themselves. The engineer observes that the distribution switch has the following setup:



```
interface VLAN 100
IP address 192.168.17.5 255.255.255.0
```

The engineer is able to reach the core router 192.168.17.1 from the distribution switch. Which of the following is the most likely cause of this issue?

Options:

A- A routing loop has occurred.

B- The subne1 mask is Incorrect.

C- The servers are not configured with default gateway.

D- There is an improper Layer 1 connection between the router and the ISP modem.

Answer:

C

Explanation:

The servers can communicate with each other but not the internet, indicating local network connectivity is fine. The distribution switch's VLAN and IP configuration are correct, and the engineer can reach the core router, suggesting the issue is not with the switch or the router. The most likely cause is that the servers do not have a default gateway configured, which is necessary for traffic to leave the local network and reach the internet.

Question 6

Question Type: MultipleChoice

Which of the following attacks can be effectively protected against by using techniques to check if a connection was made by a human user? (Select two).

Options:

A- Brute-force

B- Dictionary

C- On-path attack

D- Phishing

E- Shoulder surfing

F- Evil twin

Answer:

A, B

Explanation:

Techniques to check if a connection was made by a human user, such as CAPTCHAs, are effective against automated attacks like:

A . Brute-force: This attack method involves trying many passwords or passphrases with the hope of eventually guessing correctly.

B . Dictionary: Similar to brute-force, this attack uses a list of words to attempt to guess passwords or encryption keys.

These techniques are not designed to protect against:

C . On-path attack: Previously known as a man-in-the-middle attack, where the attacker intercepts communication between two parties.

D . Phishing: A social engineering attack aiming to trick users into giving up sensitive information.

E . Shoulder surfing: Direct observation techniques, such as looking over someone's shoulder to get information.

F . Evil twin: A rogue Wi-Fi access point that appears legitimate but is set up to eavesdrop on wireless communications.

Question 7

Question Type: MultipleChoice

Which of the following is most closely associated with the management plane?

Options:

A- Routing table

B- Current configuration

C- File operations

D- Console port

Answer:

B

Explanation:

The management plane is responsible for managing and controlling network devices. Let's evaluate the options:

Routing table: Part of the control plane, used for making forwarding decisions.

Current configuration: Part of the management plane. It includes settings, access control lists, and other configuration details.

File operations: Typically part of the management plane. It involves tasks like uploading/downloading configurations, firmware updates, and backups.

Console port: Also part of the management plane. It provides direct access to the device for configuration and troubleshooting.

Among the options, the one most closely associated with the management plane is thecurrent configuration.

Question 8

Question Type: MultipleChoice

A network engineer is installing APs for a SOHO where every staff member uses a cordless phone. Which of the following standards would work best to reduce interference?

Options:

A- 802.11a

B- 802.11b

C- 802.11g

D- 802.1X

Answer:

A

Explanation:

The network engineer is installing Access Points (APs) for a Small Office/Home Office (SOHO) where every staff member uses a cordless phone. The goal is to reduce interference. Let's evaluate the options:

802.11a: Operates in the 5 GHz frequency band. It provides higher data rates but has shorter range and poorer penetration through walls due to its higher frequency. It is less likely to interfere with cordless phones.

802.11b: Operates in the 2.4 GHz frequency band. It has slower data rates but better range and wall penetration. However, it shares the same frequency band with many cordless phones, microwave ovens, and other devices, leading to potential interference.

802.11g: Also operates in the 2.4 GHz frequency band. It provides higher data rates than 802.11b but maintains backward compatibility with 802.11b devices. Like 802.11b, it shares the same frequency band with cordless phones and other devices.

802.1X: This is not a wireless standard. It is an authentication protocol used for network access control.

Given the scenario,802.11awould work best to reduce interference because it operates in the 5 GHz band, which is less crowded and less likely to overlap with cordless phones.

Question 9

Question Type: **MultipleChoice**

A user is unable to perform a reverse DNS lookup of an IP address to a hostname. Which of the following DNS record types is missing?

Options:

A- PTR

B- CNAME

C- SOA

D- AAAA

Answer:

A

Explanation:

When a user is unable to perform a reverse DNS lookup of an IP address to a hostname, the missing DNS record type is thePTR (Pointer)record. Here's what you need to know:

PTR (Pointer) Record:

The PTR record maps an IP address to a hostname (reverse DNS lookup).

It is used to resolve IP addresses back to domain names.

For example, if you have an IP address (e.g., 192.168.1.10), the PTR record would provide the corresponding hostname (e.g., server.example.com).