N10-008 Q&As

CompTIA Network+

Pass CompTIA N10-008 Exam with 100% Guarantee

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

https://www.pass4itsure.com/n10-008.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A network administrator is implementing process changes based on recommendations following a recent penetration test. The testers used a method to gain access to the network that involved exploiting a publicly available and fixed remote code execution vulnerability in the VPN appliance. Which of the following should the administrator do to BEST prevent this from happening again?

A. Change default passwords on internet-facing hardware.

B. Implement robust ACLs with explicit deny-all entries.

C. Create private VLANs for management plane traffic.

D. Routinely upgrade all network equipment firmware.

Correct Answer: D

Firmware is the software that runs on network equipment such as routers, switches, and VPN appliances. Firmware updates often contain bug fixes, security patches, and performance improvements that can prevent or mitigate vulnerabilities and attacks. By routinely upgrading all network equipment firmware, a network administrator can ensure that the network devices are running the latest and most secure versions of firmware and avoid exploiting known and fixed remote code execution vulnerabilities in the VPN appliance.

References: https://www.comptia.org/training/books/network-n10-008-study-guide (page 462)

QUESTION 2

During the security audit of a financial firm the Chief Executive Officer (CEO) questions why there are three employees who perform very distinct functions on the server. There is an administrator for creating users another for assigning the

users lo groups and a third who is the only administrator to perform file rights assignment.

Which of the following mitigation techniques is being applied\\'

A. Privileged user accounts

B. Role separation

C. Container administration

D. Job rotation

Correct Answer: B

Role separation is a security principle that involves dividing the tasks and privileges for a specific business process among multiple users. This reduces the risk of fraud and errors, as no one user has complete control over the process. In the scenario, there are three employees who perform very distinct functions on the server, which is an example of role separation. References: https://hyperproof.io/resource/segregation-of-duties/

QUESTION 3

Which of the following attacks MOST likely utilizes a botnet to disrupt traffic?

A. DDoS

B. Deauthentication

C. Social engineering

D. Ransomware

E. DNS poisoning

Correct Answer: A

QUESTION 4

Branch users are experiencing issues with videoconferencing. Which of the following will the company MOST likely configure to improve performance for these applications?

A. Link Aggregation Control Protocol

B. Dynamic routing

C. Quality of service

D. Network load balancer

E. Static IP addresses

Correct Answer: C

QUESTION 5

Users are reporting performance issues when attempting to access the main fileshare server. Which of the following steps should a network administrator perform next based on the network troubleshooting methodology?

A. Implement a fix to resolve the connectivity issues.

B. Determine if anything has changed.

C. Establish a theory of probable cause.

D. Document all findings, actions, and lessons learned.

Correct Answer: B

According to the network troubleshooting methodology, the first step is to identify the problem and gather information about the current state of the network using the network troubleshooting tools that are available1. The next step is to determine if anything has changed in the network configuration, environment, or usage that could have caused or contributed to the performance issues1. This step helps to narrow down the possible causes and eliminate irrelevant factors. For example, the network administrator could check if there were any recent updates, patches, or modifications to the fileshare server or the network devices that connect to it. They could also check if there was an increase in network traffic or demand for the fileshare server resources2. The other options are not correct because they are not the

next steps in the network troubleshooting methodology. Implementing a fix to resolve the connectivity issues (A) is premature without determining the root cause of the problem. Establishing a theory of probable cause ?is a later step that requires testing and verification. Documenting all findings, actions, and lessons learned (D) is the final step that should be done after resolving the problem and restoring normal network operations1.