# 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**

Which of the following would be the MOST likely attack used to bypass an access control vestibule?

A. Tailgating

B. Phishing

C. Evil twin

D. Brute-force

Correct Answer: A

Tailgating is when someone follows an authorized person into a restricted area without having the proper credentials. This is usually done by pretending to be with the authorized person, or by offering assistance. Tailgating is a social engineering attack and does not require any technical skill.

**QUESTION 3**

A network administrator wants to improve the security of the management console on the company\\'s switches and ensure configuration changes made can be correlated to the administrator who conformed them. Which of the following should the network administrator implement?

A. Port security

B. Local authentication

C. TACACS+

D. Access control list

Correct Answer: C

TACACS+ is a protocol that provides centralized authentication, authorization, and accounting (AAA) for network devices and users. TACACS+ can help improve the security of the management console on the company\\'s switches by verifying the identity and credentials of the administrators, enforcing granular access policies and permissions, and logging the configuration changes made by each administrator. This way, the network administrator can ensure only authorized and authenticated users can access and modify the switch settings, and also track and correlate the changes made by each user. References: https://www.comptia.org/blog/what-is-tacacs

**QUESTION 4**

Which of the following is an example of on-demand scalable hardware that is typically housed in the vendor\\'s data center?

A. DaaS

B. IaaS

C. PaaS

D. SaaS

Correct Answer: B

**QUESTION 5**

A user has called the help desk with a problem reaching certain servers within the organization. The organization is using RFC 1819 for internal networks. The servers having trouble are configured with the following IP addresses: 192. 130.

135. 5 and 192. 130. 135. 6.

The user cannot connect to the correct servers. Which of the following explain why this is happening to the user?

A. The network has been configured with an inappropriate scheme

B. The serves are periodical/ going offline and rejecting the connection.

C. The default route in the user\\'s computer points to the wrong upstream device.

D. The IPS system is flagging the traffic as suspicious and terminating the connection.

Correct Answer: A