N10-008 Q&As

CompTIA Network+

Pass CompTIA N10-008 Exam with 100% Guarantee

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

QUESTION 1

Which of the following would be BEST to use to detect a MAC spoofing attack?

A. Internet Control Message Protocol

B. Reverse Address Resolution Protocol

C. Dynamic Host Configuration Protocol

D. Internet Message Access Protocol

Correct Answer: B

Reverse Address Resolution Protocol . Can be used to ask what a machine\\'s IP address is based on it\\'s MAC address. If the adress has been spoofed it will obviously show a different IP than the one it is expecting to see

QUESTION 2

A network administrator is required to ensure that auditors have read-only access to the system logs, while systems administrators have read and write access to the system logs, and operators have no access to the system logs. The network administrator has configured security groups for each of these functional categories. Which of the following security capabilities will allow the network administrator to maintain these permissions with the LEAST administrative effort?

A. Mandatory access control

B. User-based permissions

C. Role-based access

D. Least privilege

Correct Answer: C

Role-based access is a security capability that assigns permissions to users based on their roles or functions within an organization. It allows the network administrator to maintain these permissions with the least administrative effort, as they only need to configure the security groups for each role once and then assign users to those groups. Mandatory access control is a security capability that assigns permissions based on security labels or classifications, which requires more administrative effort to maintain. User-based permissions are a security capability that assigns permissions to individual users, which is not scalable or efficient for large organizations. Least privilege is a security principle that states that users should only have the minimum level of access required to perform their tasks, which is not a security capability by itself.

QUESTION 3

A company\\'s web server is hosted at a local ISP. This is an example of:

A. colocation

B. an on-premises data center.

C. a branch office.

D. a cloud provider.

Correct Answer: A

Colocation refers to the practice of housing privately-owned servers and networking equipment in a third-party data center facility. In this scenario, the company\\'s web server is hosted at a local ISP, which means that the server is physically located at the ISP\\'s data center facility and is not on-premises at the company\\'s own facility. The company likely rents rack space, power, cooling, and network connectivity from the ISP to house their server.

On-premises data center refers to a company-owned facility that houses its own servers and networking equipment. A branch office is a remote location of a company, typically with its own set of IT resources. A cloud provider refers to a third-party company that provides cloud computing services, which typically involve hosting applications and data in the provider\\'s data center facilities.

QUESTION 4

A network administrator has been directed to present the network alerts from the past week to the company\\'s executive staff. Which of the following will provide the BEST collection and presentation of this data?

A. A port scan printout

B. A consolidated report of various network devices

C. A report from the SIEM tool

D. A report from a vulnerability scan done yesterday

Correct Answer: C

SIEM stands for Security Information and Event Management, which is a tool that collects, analyzes, and correlates data from various network devices and sources to provide alerts and reports on security incidents and events. A report from the SIEM tool can provide a comprehensive overview of the network alerts from the past week to the executive staff, highlighting any potential threats, vulnerabilities, or anomalies. References: https://www.comptia.org/blog/what-is-siem

QUESTION 5

An auditor assessing network best practices was able to connect a rogue switch into a network Jack and get network connectivity. Which of the following controls would BEST address this risk?

A. Activate port security on the switchports providing end user access.

B. Deactivate Spanning Tree Protocol on network interfaces that are facing public areas.

C. Disable Neighbor Resolution Protocol in the Layer 2 devices.

D. Ensure port tagging is in place for network interfaces in guest areas

Correct Answer: A

Activate port security on the switchports providing end user access would BEST address the risk of a rogue switch being connected to the network. Port security limits the number of devices that can connect to a particular switchport, thereby preventing unauthorized devices from connecting to the network. By limiting the number of MAC addresses allowed on each switchport, the network administrator can help prevent rogue devices from connecting and potentially causing security issues.