SK0-005Q&As

CompTIA Server+ Certification Exam

Pass CompTIA SK0-005 Exam with 100% Guarantee

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

https://www.passapply.com/sk0-005.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A security administrator ran a port scanning tool against a virtual server that is hosting a secure website. A list of open ports was provided as documentation. The management team has requested that non-essential ports be disabled on the firewall. Which of the following ports must remain open?

A. 25

B. 53

C. 443

D. 3389

E. 8080

Correct Answer: C

QUESTION 2

A server administrator has been asked to implement a password policy that will help mitigate the chance of a successful brute-force attack. Which of the following password policies should the administrator implement first?

A. Lockout

B. Length

C. Complexity

D. Minimum age

Correct Answer: A

QUESTION 3

An administrator is investigating several unexpected documents and video files that recently appeared in a network share. The administrator checks the properties of the files and sees the author\\'s name on the documents is not a company employee. The administrator questions the other users, but no one knows anything about the files. The administrator then checks the log files and discovers the FTP protocol was used to copy the files to the server.

Which of the following needs to be done to prevent this from happening again?

A. Implement data loss prevention.

B. Configure intrusion detection.

C. Turn on User Account Control.

D. Disable anonymous access.

Correct Answer: D

D. Disable anonymous access.

The fact that the FTP protocol was used to copy the files to the server suggests that the network share has anonymous access enabled. Disabling anonymous access would require users to authenticate before accessing the share, which would prevent unauthorized access and file transfers from external sources.

Data loss prevention (A) and intrusion detection (B) are both important security measures, but they may not necessarily prevent unauthorized access to a network share. User Account Control (C) is a feature in Windows that helps prevent unauthorized changes to a computer, but it is not directly related to preventing unauthorized access to a network share. Therefore, the best option in this scenario would be to disable anonymous access.

QUESTION 4

Joe, a user in the IT department, cannot save changes to a sensitive file on a Linux server. An is -la shows the following listing: -rw-r--r 1 Ann IT 6780 12 June 2019 filename

Which of the following commands would BEST enable the server technician to allow Joe to have access without granting excessive access to others?

A. chmod 777 filename

B. chown Joe filename

C. chmod g+w filename

D. chgrp IT filename

Correct Answer: C

QUESTION 5

Which of the following should be configured in pairs on a server to provide network redundancy?

A. MRU

B. SCP

C. DLP

D. CPU

E. NIC

Correct Answer: E

The network component that should be configured in pairs on a server to provide network redundancy is the NIC (Network Interface Card).

NIC redundancy can be achieved by installing two NICs on a server and configuring them in a team or bond. This allows for the NICs to work in tandem and provide redundancy in case one of the NICs fails or experiences issues. If one NIC fails, the other NIC can continue to handle the network traffic, which helps to ensure that the server remains connected to the network and available.

While other components listed may have redundancy options or configurations, they do not provide network redundancy in pairs on a server. MRU (Maximum Receive Unit) is a networking term that refers to the largest size of a packet that can be received on a network interface. SCP (Secure Copy Protocol) is a protocol used for securely transferring files between systems. DLP (Data Loss Prevention) is a strategy or technology used to prevent the loss or theft of sensitive data. CPU (Central Processing Unit) is a hardware component that processes instructions in a computer.