Free Questions for SK0-005 by actualtestdumps

Shared by Bush on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The network's IDS is giving multiple alerts that unauthorized traffic from a critical application server is being sent to a known-bad public IP address.

One of the alerts contains the following information:

Exploit Alert

Attempted User Privilege Gain

2/2/07-3: 09:09 10.1.200.32

--> 208.206.12.9:80

This server application is part of a cluster in which two other servers are also servicing clients. The server administrator has verified the other servers are not sending out traffic to that public IP address. The IP address subnet of the application servers is 10.1.200.0/26. Which of the following should the administrator perform to ensure only authorized traffic is being sent from the application server and downtime is minimized? (Select two).

Options:

A) Disable all services on the affected application server.

B) Perform a vulnerability scan on all the servers within the cluster and patch accordingly.

C) Block access to 208.206.12.9 from all servers on the network.

D) Change the IP address of all the servers in the cluster to the 208.206.12.0/26 subnet.

E) Enable GPO to install an antivirus on all the servers and perform a weekly reboot.

F) Perform an antivirus scan on all servers within the cluster and reboot each server.

Answer:

B, F

Explanation:

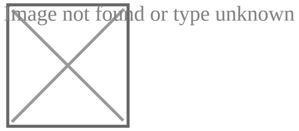
The administrator should perform an antivirus scan on all servers within the cluster and reboot each server, and block access to 208.206.12.9 from all servers on the network. These actions will help to remove any malware that may have infected the application server and prevent any further unauthorized traffic to the known-bad public IP address. An antivirus scan can detect and remove malicious software that may be sending data to an external source, and a reboot can clear any temporary files or processes that may be related to the malware. Blocking access to 208.206.12.9 from all servers on the network can prevent any future attempts to communicate with the malicious IP address.

References:CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.4, Objective 3.4; Chapter 6, Lesson 6.2, Objective 6.2

Question 2

Question Type: MultipleChoice

Refer to exihibit:



Which of the following actions should the server administrator perform on the server?

Options:

A) Close ports 69 and 1010 and rerun the scan.

B) Close ports 80 and 443 and rerun the scan.

C) Close port 3389 and rerun the scan.

D) Close all ports and rerun the scan.

Answer:

C

Explanation:

The server administrator should close port 3389 and rerun the scan. Port 3389 is used for Remote Desktop Protocol (RDP), which allows remote access and control of a server. RDP is vulnerable to brute-force attacks, credential theft, and malware infection. Closing port 3389 can prevent unauthorized access and improve the security of the server. The other ports are not as risky as port 3389 and can be left open for legitimate purposes.Reference:CompTIA Server+ Certification Exam Objectives, Domain 5.0: Security, Objective 5.4: Given a scenario, implement proper environmental controls and techniques.

Question 3

Question Type: **MultipleChoice**

A technician is attempting to reboot a remote physical Linux server. However, attempts to command a shutdown -----now result in the loss of the SSH connection. The server still responds to pings. Which of the following should the technician use to command a remote shutdown?

A virtual serial console

Options:

B) A KVM

C) An IDRAC

D) A crash cart

Answer:

C

Explanation:

An IDRAC (Integrated Dell Remote Access Controller) is a tool that can be used to command a remote shutdown of a physical Linux server. An IDRAC is a hardware device that provides out-of-band management for Dell servers. It allows the technician to access the server's console, power cycle, reboot, or shut down the server remotely using a web interface or a command-line interface. An IDRAC does not depend on the operating system or network connectivity of the server. A virtual serial console is a tool that can be used to access a remote virtual machine's console using a serial port connection. A KVM (Keyboard, Video, Mouse) switch is a device that allows the technician to switch between different computer sources using the same keyboard, monitor, and mouse. A crash cart is a mobile unit that contains a keyboard, monitor, mouse, and other tools that can be connected to a physical server for troubleshooting purposes. Reference: https://www.dell.com/support/kbdoc/en-us/000131486/understanding-the-idrac https://www.howtogeek.com/799968/what-is-a-kvm-switch/ https://www.techopedia.com/definition/1032/business-impact-analysis-bia

Question 4

Question Type: **MultipleChoice**

The network's IDS is giving multiple alerts that unauthorized traffic from a critical application server is being sent to a known-bad public IP address.

One of the alerts contains the following information:

Exploit Alert

Attempted User Privilege Gain

2/2/07-3: 09:09 10.1.200.32

--> 208.206.12.9:80

This server application is part of a cluster in which two other servers are also servicing clients. The server administrator has verified the other servers are not sending out traffic to that public IP address. The IP address subnet of the application servers is 10.1.200.0/26. Which of the following should the administrator perform to ensure only authorized traffic is being sent from the application server and downtime is minimized? (Select two).

Options:

A) Disable all services on the affected application server.

B) Perform a vulnerability scan on all the servers within the cluster and patch accordingly.

C) Block access to 208.206.12.9 from all servers on the network.

D) Change the IP address of all the servers in the cluster to the 208.206.12.0/26 subnet.

E) Enable GPO to install an antivirus on all the servers and perform a weekly reboot.

F) Perform an antivirus scan on all servers within the cluster and reboot each server.

Answer:

B, F

Explanation:

The administrator should perform an antivirus scan on all servers within the cluster and reboot each server, and block access to 208.206.12.9 from all servers on the network. These actions will help to remove any malware that may have infected the application server and prevent any further unauthorized traffic to the known-bad public IP address. An antivirus scan can detect and remove malicious software that may be sending data to an external source, and a reboot can clear any temporary files or processes that may be related to the malware. Blocking access to 208.206.12.9 from all servers on the network can prevent any future attempts to communicate with the malicious IP address.

References:CompTIA Server+ SK0-005 Certification Study Guide, Chapter 3, Lesson 3.4, Objective 3.4; Chapter 6, Lesson 6.2, Objective 6.2

Question 5

Question Type: **MultipleChoice**

Refer to exihibit:

Image not found or type unknown

Which of the following actions should the server administrator perform on the server?

Options:

A) Close ports 69 and 1010 and rerun the scan.

B) Close ports 80 and 443 and rerun the scan.

C) Close port 3389 and rerun the scan.

D) Close all ports and rerun the scan.

Answer:

C

Explanation:

The server administrator should close port 3389 and rerun the scan. Port 3389 is used for Remote Desktop Protocol (RDP), which allows remote access and control of a server. RDP is vulnerable to brute-force attacks, credential theft, and malware infection. Closing port 3389 can prevent unauthorized access and improve the security of the server. The other ports are not as risky as port 3389 and can be left open for legitimate purposes.Reference:CompTIA Server+ Certification Exam Objectives, Domain 5.0: Security, Objective 5.4: Given a scenario, implement proper environmental controls and techniques.

Question 6

Question Type: MultipleChoice

Users report they ate unable to access an application after a recent third-party patch update. The physical server that is hosting the application keeps crashing on reboot. Although the update was installed directly from the manufacturer's support website as recommended it has now been recalled and removed from the website as the update unintentionally installed unauthorized software after a reboot. Which of the following steps should the administrator perform to restore access to the application while minimizing downtime? (Select TWO)

a. Uninstall recent updates.

Options:

B) Reimage the server with a different OS.

C) Run a port scan to verify open ports.

D) Enable a GPO to uninstall the update.

E) Scan and remove any malware.

F) Reformat the server and restore the image from the latest backup.

Answer:

E, F

Explanation:

The most likely cause of the server crashing and the application being inaccessible is that the unauthorized software installed by the update is malware that corrupted the system files or compromised the security of the server. To restore access to the application while minimizing downtime, the administrator should scan and remove any malware from the server, and then reformat the server and restore the image from the latest back-up. This will ensure that the server is clean and has a working configuration of the application. Verified Reference: [How to Remove Malware from a Server]

Question 7

Question Type: MultipleChoice

Which of the following BEST describes a warm site?

The site has all infrastructure and live data.

Options:

B) The site has all infrastructure and some data

C) The site has partially redundant infrastructure and no network connectivity

D) The site has partial infrastructure and some data.

Answer:

D

Explanation:

A warm site is a type of disaster recovery site that has some pre-installed hardware, software, and network connections, but not as much as a hot site. A warm site also has some backup data, but not as current as a hot site. A warm site requires some time and effort to become fully operational in the event of a disaster. A hot site is a disaster recovery site that has all infrastructure and live data, and can take over the primary site's operations immediately. A cold site is a disaster recovery site that has no infrastructure or data, and requires significant time and resources to set up. Reference:

https://www.enterprisestorageforum.com/management/disaster-recovery-site/

https://www.techopedia.com/definition/3780/warm-site

Question 8

Question Type: MultipleChoice

A server administrator is exporting Windows system files before patching and saving them to the following location:

Which of the following is a storage protocol that the administrator is MOST likely using to save this data?

Options:

A) eSATA

B) FCoE

C) CIFS

D) SAS

Answer:

C

Question 9

Question Type: MultipleChoice

A server technician has been asked to upload a few files from the internal web server to the internal FTP server. The technician logs in to the web server using PuTTY, but the connection to the FTP server fails. However, the FTP connection from the technician's workstation is sucessful. To troubleshoot the issue, the technician executes the following command on both the web server and the workstation:

The IP address in the command output is different on each machine. Which of the following is the MOST likely reason for the connection failure?

Options:

A) A misconfigured firewall

B) A misconfigured hosts.deny file

C) A misconfigured hosts file

D) A misconfigured hosts.allow file

Answer:

D