Free Questions for XK0-005 by certsdeals

Shared by Hammond on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A Linux administrator has physically added a new RAID adapter to a system. Which of the following commands should the Linux administrator run to confirm that the device has been recognized? (Select TWO).

Options:

A- rmmod

B- Is -11 /etc

C- Ishw ---class disk

D- pvdisplay

E- rmdir /dev

F- dmesg

Answer:

C, F

Explanation:

The following commands can help you confirm that the new RAID adapter has been recognized by the Linux system:

dmesg: This command displays the kernel messages, which can show the information about the newly detected hardware device. You can usedmesg | grep -i raidto filter the output for RAID-related messages.

lshw -class disk: This command lists the disk devices on the system, including the RAID controller and its model name.You can uselshw -class disk | grep -i raidto filter the output for RAID-related information1.

The other commands are not relevant for this purpose. For example:

rmmod: This command removes a module from the Linux kernel, which is not useful for detecting a new device.

ls -l /etc: This command lists the files and directories in the /etc directory, which is not related to hardware devices.

pvdisplay: This command displays the attributes of physical volumes, which are part of the logical volume management (LVM) system, not the RAID system.

rmdir /dev: This command removes an empty directory, which is not helpful for detecting a new device. Moreover, /dev is a special directory that contains device files, and should not be removed.

Question 2

Question Type: **MultipleChoice**

During a security scan, the password of an SSH key file appeared to be too weak and was cracked. Which of the following commands would allow a user to choose a stronger password and set it on the existing SSH key file?

Options:

A- passwd

B- ssh

C- ssh-keygen

D- pwgen

Answer:

C

Explanation:

The command that would allow a user to choose a stronger password and set it on the existing SSH key file is ssh-keygen -p -f <keyfile>. This command uses the ssh-keygen tool, which is used to generate, manage, and convert authentication keys for SSH. The -p option stands for passphrase, and it allows the user to change or remove the passphrase of an existing private key file. The -f option specifies the filename of the key file. The command will prompt the user for the old passphrase, and then for the new passphrase twice.

The other options are not correct commands for changing the password of an SSH key file. The passwd command is used to change the password of a user account on a Linux system, not an SSH key file. The ssh command is used to log in to a remote system using SSH,

not to change the password of an SSH key file. The pwgen command is used to generate random passwords, not to change the password of an SSH key file.

Question 3

Question Type: MultipleChoice

What is the main objective when using Application Control?

Options:

A- To filter out specific content.

B- To assist the firewall blade with handling traffic.

C- To see what users are doing.

D- Ensure security and privacy of information.

Answer:

D

Explanation:

The main objective when using Application Control is to ensure the security and privacy of information. Application Control is a security practice that blocks or restricts unauthorized applications from executing in ways that put data at risk.The control functions vary based on the business purpose of the specific application, but the main objective is to help ensure the privacy and security of data used by and transmitted between applications1.Application Control can also prevent malware, untrusted, or unwanted applications from running on the network, reducing the risks and costs associated with data breaches1.Application Control can also improve the overall network stability and performance by eliminating unnecessary or harmful applications1.

Application Control is not mainly used to filter out specific content, although it can be combined with other technologies such as URL filtering or content filtering to achieve that goal. Application Control is not mainly used to assist the firewall blade with handling traffic, although it can be integrated with firewall policies to enforce granular access rules based on applications. Application Control is not mainly used to see what users are doing, although it can provide visibility and reporting on application usage and activity.

Question 4

Question Type: MultipleChoice

Using AD Query, the security gateway connections to the Active Directory Domain Controllers using what protocol?

Options:

A- Windows Management Instrumentation (WMI)

B- Hypertext Transfer Protocol Secure (HTTPS)

C- Lightweight Directory Access Protocol (LDAP)

D- Remote Desktop Protocol (RDP)

Answer:

C

Explanation:

Using AD Query, the security gateway connects to the Active Directory Domain Controllers using Lightweight Directory Access Protocol (LDAP). LDAP is a protocol that provides access to directory services over a network. AD Query uses LDAP queries to retrieve information about users and groups from Active Directory Domain Controllers without installing any software on them. AD Query does not use Windows Management Instrumentation (WMI), Hypertext Transfer Protocol Secure (HTTPS), or Remote Desktop Protocol (RDP) to connect to Active Directory Domain Controllers.Reference:Check Point Certified Security Administrator (CCSA) R80.x Study Guide, Chapter 5: User Management and Authentication, page 69.

Question 5

Question Type: MultipleChoice

Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use which operating system?

Options:

A- Centos Linux

B- Gaia embedded

C- Gaia

D- Red Hat Enterprise Linux version 5

Answer:

B

Explanation:

Rugged appliances are small appliances with ruggedized hardware that use Gaia embedded as their operating system. Gaia embedded is a version of Gaia that is optimized for embedded devices such as Rugged appliances and Quantum Spark appliances. Gaia embedded supports features such as VPN, firewall, identity awareness, application control, URL filtering, and anti-bot. Gaia embedded does not use Centos Linux, Gaia, or Red Hat Enterprise Linux version 5 as their operating system.Reference:Check Point Rugged Appliance Datasheet, page 1.

Question 6

Question Type: MultipleChoice

At what point is the Internal Certificate Authority (ICA) created?

Options:

A- During the primary Security Management Server installation process.

B- Upon creation of a certificate.

C- When an administrator decides to create one.

D- When an administrator initially logs into SmartConsole.

Answer:

A

Explanation:

The Internal Certificate Authority (ICA) is created during the primary Security Management Server installation process. The ICA is a component of Check Point's Public Key Infrastructure (PKI) that issues and manages certificates for Security Gateways and administrators. The ICA is automatically installed and initialized when the primary Security Management Server is installed. The ICA is not created upon creation of a certificate, when an administrator decides to create one, or when an administrator initially logs into SmartConsole.Reference:Check Point Certified Security Administrator (CCSA) R80.x Study Guide, Chapter 3: Check Point Security Management Architecture, page 32.

Question 7

Question Type: MultipleChoice

A database administrator requested the installation of a custom database on one of the servers. Which of the following should the Linux administrator configure so the requested packages can be installed?

Options:

A- /etc/yum.conf

B- /etc/ssh/sshd.conf

C- /etc/yum.repos.d/db.repo

D- /etc/resolv.conf

Answer:

C

Explanation:

The Linux administrator should configure /etc/yum.repos.d/db.repo so that the requested packages can be installed. This file defines a custom repository for yum, which is a package manager for RPM-based systems. The file should contain information such as the name, baseurl, gpgcheck, and enabled options for the repository. By creating this file and enabling the repository, the administrator can use yum to install packages from the custom repository. The /etc/yum.conf file is the main configuration file for yum, but it does not define repositories. The /etc/ssh/sshd.conf file is the configuration file for sshd, which is a daemon that provides secure shell access to remote systems. The /etc/resolv.conf file is the configuration file for DNS resolution, which maps domain names to IP addresses.Reference:CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Packages and Software, page 559.