Free Questions for XK0-005 by dumpshq

Shared by Austin on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A Linux administrator needs to connect securely to a remote server in order to install application software. Which of the following commands would allow this connection?

Options:

A- scp 'ABC-key.pem' root@10.0.0.1

B- sftp rooteiO.0.0.1

C- telnet 10.0.0.1 80

D- ssh -i 'ABC-key.pem' root@10.0.0.1

E- sftp 'ABC-key.pem' root@10.0.0.1

Answer:

D

Explanation:

The commandssh -i 'ABC-key.pem' root@10.0.0.1would allow the administrator to connect securely to the remote server in order to install application software. Thesshcommand is a tool for establishing secure and encrypted connections between remote systems. The-ioption specifies the identity file that contains the private key for key-based authentication. The'ABC-key.pem'is the name of the identity file that contains the private key. Theroot@10.0.0.1is the username and the IP address of the remote server. The commandssh -i 'ABC-key.pem' root@10.0.0.1will connect to the remote server using the private key and allow the administrator to install application software. This is the correct command to use to connect securely to the remote server. The other options are incorrect because they either do not use key-based authentication (sftp root@10.0.0.1ortelnet 10.0.0.1 80) or do not use the correct syntax for the command (scp 'ABC-key.pem' root@10.0.0.1instead ofscp -i 'ABC-key.pem' root@10.0.0.1orsftp 'ABC-key.pem' root@10.0.0.1instead ofsftp -i 'ABC-key.pem' root@10.0.0.1).Reference:CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 17: Implementing Basic Security, page 513.

Question 2

Question Type: MultipleChoice

A Linux engineer receives reports that files created within a certain group are being modified by users who are not group members. The engineer wants to reconfigure the server so that only file owners and group members can modify new files by default. Which of the following commands would accomplish this task?

Options:

A- chmod 775

B- umask. 002

C- chactr -Rv

D- chown -cf

Answer:

B

Explanation:

The commandumask 002will accomplish the task of reconfiguring the server so that only file owners and group members can modify new files by default. Theumaskcommand is a tool for setting the default permissions for new files and directories on Linux systems. The umask value is a four-digit octal number that represents the permissions that are subtracted from the default permissions. The default permissions for files are 666, which means read and write for owner, group, and others. The default permissions for directories are 777, which means read, write, and execute for owner, group, and others. The umask value consists of four digits: the first digit is for special permissions, such as setuid, setgid, and sticky bit; the second digit is for the owner permissions; the third digit is for the group permissions; and the fourth digit is for the others permissions. The umask value can be calculated by subtracting the desired permissions from the default permissions. For example, if the desired permissions for files are 664, which means read and write for owner and group, and read for others, then the umask value is 002, which is 666 - 664. The commandumask 002will set the umask value to 002, which will ensure that only file owners and group members can modify new files by default. This is the correct command to use to accomplish the task. The other options are incorrect because they either do not set the default permissions for new files (chmod 775orchown -cf) or do not exist (chattr -Rv).Reference:CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing File Permissions and Ownership, page 349.

Question 3

Question Type: MultipleChoice

The security team has identified a web service that is running with elevated privileges A Linux administrator is working to change the systemd service file to meet security compliance standards. Given the following output:

```
[Unit]
Description=CompTIA server daemon
Documentation=man:webserver(8) man:webserver_config(5)
After=network.target

[Service]
Type=notify
EnvironmentFile=/etc/webserver/config
ExecStart=/usr/sbin/webserver -D $OPTIONS
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartSec=42s

[Install]
WantedBy=multi-user.target
```

Which of the following remediation steps will prevent the web service from running as a privileged user?

Options:

A- Removing the ExecStarWusr/sbin/webserver -D SOPTIONS from the service file

B- Updating the Environment File line in the [Service] section to/home/webservice/config

C- Adding the User-webservice to the [Service] section of the service file

D- Changing the:nulti-user.target in the [Install] section to basic.target

Answer:

C

Explanation:

The remediation step that will prevent the web service from running as a privileged user is adding the User=webservice to the [Service] section of the service file. The service file is a configuration file that defines the properties and behavior of a systemd service. The systemd is a system and service manager that controls the startup and operation of Linux systems. The service file contains various sections and options that specify how the service should be started, stopped, and managed. The [Service] section defines how the service should be executed and what commands should be run. The User option specifies the user name or ID that the service should run as. The webservice is the name of the user that the administrator wants to run the web service as. The administrator should add the User=webservice to the [Service] section of the service file, which will prevent the web service from running as a privileged user, such as root, and improve the security of the system. This is the correct remediation step to use to prevent the web service from running as a privileged user. The other options are incorrect because they either do not change the user that the service runs as (removing the

ExecStart=/usr/sbin/webserver -D OPTIONS from the service fileorupdating the EnvironmentFile line in the [Service] section to /home/webservice/config) or do not affect the user that the service runs as (changing the multi-user.target in the [Install] section to basic.target).Reference:CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 15: Managing System Services, page 458.

Question 4

Question Type: MultipleChoice

In order to copy data from another VLAN, a systems administrator wants to temporarily assign IP address 10.0.6 5/24 to the newly added network interface enp1s0f1. Which of the following commands should the administrator run to achieve the goal?

Options:

A- ip addr add 10.0.6.5/24 dev enpls0f1

B- echo 'IPV4_ADDRESS=10.0.6.5/24' > /etc/sysconfig/network-scripts/ifcfg-enplsOfl

C- ifconfig 10.0.6.5/24 enpsIs0f1

D- nmcli conn add lpv4.address-10.0.6.5/24 ifname enpls0f1

Answer:

A

Explanation:

The commandip addr add 10.0.6.5/24 dev enp1s0f1will achieve the goal of temporarily assigning IP address 10.0.6.5/24 to the newly added network interface enp1s0f1. Theipcommand is a tool for managing network interfaces and routing on Linux systems. Theaddroption specifies the address manipulation mode. Theaddoption adds a new address to an interface. The10.0.6.5/24is the IP address and the subnet mask in CIDR notation. Thedevoption specifies the device name. Theenp1s0f1is the name of the network interface. The commandip addr add 10.0.6.5/24 dev enp1s0f1will add the IP address 10.0.6.5/24 to the network interface enp1s0f1, which will allow the administrator to copy data from another VLAN. This is the correct command to use to achieve the goal. The other options are incorrect because they either do not add a new address to an interface (echo 'IPV4_ADDRESS=10.0.6.5/24' > /etc/sysconfig/network-scripts/ifcfg-enp1s0f1orifconfig 10.0.6.5/24 enp1s0f1) or do not use the correct syntax for the command (nmcli conn add ipv4.address-10.0.6.5/24 ifname enp1s0f1instead ofnmcli conn add type ethernet ipv4.address 10.0.6.5/24 ifname enp1s0f1).Reference:CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 12: Managing Network Connections, page 385.

Question 5

Question Type: MultipleChoice

An administrator recently updated the BIND software package and would like to review the default configuration that shipped with this version. Which of the following files should the administrator review?

Options:

A- /etc/named.conf.rpmnew

B- /etc/named.conf.rpmsave

C- /etc/named.conf

D- /etc/bind/bind.conf

Answer:

A

Explanation:

After installing a new version of a package that includes a configuration file that already exists on the system, such as /etc/httpd/conf/httpd.conf, RPM will create a new file with the .rpmnew extension instead of overwriting the existing file. This allows the administrator to review the default configuration that shipped with this version and compare it with the current configuration before deciding whether to merge or replace the files. The /etc/named.conf.rpmsave file is created by RPM when a package is uninstalled and it contains a configuration file that was modified by the administrator. This allows the administrator to restore the configuration file if needed. The /etc/named.conf file is the main configuration file for the BIND name server, not the httpd web server. The /etc/bind/bind.conf file does not exist by default in Linux systems.Reference:CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Packages and Software, page 561.

Question 6

Question Type: MultipleChoice

After installing a new version of a package, a systems administrator notices a new version of the corresponding, service file was Installed In order to use the new version of the, service file, which of the following commands must be Issued FIRST?

Options:

A- systemctl status

B- systemctl stop

C- systemctl reinstall

D- systemctl daemon-reload

Answer:

D

Explanation:

After installing a new version of a package that includes a new version of the corresponding service file, the systemctl daemon-reload command must be issued first in order to use the new version of the service file. This command will reload the systemd manager

configuration and read all unit files that have changed on disk. This will ensure that systemd recognizes the new service file and applies its settings correctly. The systemctl status command will display information about a service unit, but it will not reload the configuration. The systemctl stop command will stop a service unit, but it will not reload the configuration. The systemctl reinstall command does not exist.Reference:CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 17: System Maintenance and Operation, page 518.