XK0-005$^{Q\&As}$

CompTIA Linux+ Certification Exam

Pass CompTIA XK0-005 Exam with 100% Guarantee

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

QUESTION 1

A new disk was presented to a server as /dev/ sdd. The systems administrator needs to check if a partition table is on that disk. Which of the following commands can show this information?

A. Isscsi

B. fdisk

C. blkid

D. partprobe

Correct Answer: B

Explanation: The command that can be used to check if a partition table is on a disk is fdisk. The fdisk command can display, create, delete, and modify partitions on a disk. To show the partition table of a disk, the administrator can use fdisk -l

/dev/sdd (B).

References:

[CompTIA Linux+ Study Guide], Chapter 5: Managing Filesystems and Logical Volumes, Section: Partitioning Disks

[How to Use Fdisk Command in Linux]

QUESTION 2

A systems administrator is tasked with creating an Ansible playbook to automate the installation of patches on several Linux systems. In which of the following languages should the playbook be written?

A. SQL

B. YAML

C. HTML

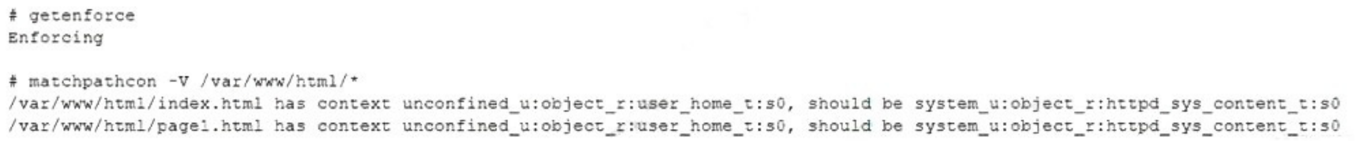
D. JSON

Correct Answer: B

Explanation: The language that the playbook should be written in is YAML. YAML stands for YAML Ain\\'t Markup Language, which is a human-readable data serialization language. YAML is commonly used for configuration files and data exchange. YAML uses indentation, colons, dashes, and brackets to represent the structure and values of the data. YAML also supports comments, variables, expressions, and functions. Ansible is an open-source tool for automating tasks and managing configuration on Linux systems. Ansible uses YAML to write playbooks, which are files that define the desired state and actions for the systems. Playbooks can be used to automate the installation of patches on several Linux systems by specifying the hosts, tasks, modules, and parameters. The language that the playbook should be written in is YAML. This is the correct answer to the question. The other options are incorrect because they are not the languages that Ansible uses for playbooks (SQL, HTML, or JSON). References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Securing Linux Systems, page 549.

QUESTION 3

A Linux systems administrator is setting up a new web server and getting 404 - NOT FOUND errors while trying to access the web server pages from the browser. While working on the diagnosis of this issue, the Linux systems administrator executes the following commands:



```
# getenforce
Enforcing

# matchpathcon -V /var/www/html/*
/var/www/html/index.html has context unconfined_u:object_r:user_home_t:s0, should be system_u:object_r:httpd_sys_content_t:s0
/var/www/html/page1.html has context unconfined_u:object_r:user_home_t:s0, should be system_u:object_r:httpd_sys_content_t:s0
```

Which of the following commands will BEST resolve this issue?

A. sed -i \\'s/SELINUX=enforcing/SELINUX=disabled/\\' /etc/selinux/config

B. restorecon -R -v /var/www/html

C. setenforce 0

D. setsebool -P httpd_can_network_connect_db on

Correct Answer: B

Explanation: The command restorecon -R -v /var/www/html will best resolve the issue. The issue is caused by the incorrect SELinux context of the web server files under the /var/www/html directory. The output of ls -Z /var/www/html shows that the files have the type user_home_t, which is not allowed for web content. The command restorecon restores the default SELinux context of files based on the policy rules. The options -R and -v are used to apply the command recursively and verbosely. This command will change the type of the files to httpd_sys_content_t, which is the correct type for web content. This will allow the web server to access the files and serve the pages to the browser. The other options are incorrect because they either disable SELinux entirely (sed -i \\'s/SELINUX=enforcing/SELINUX=disabled/\\' /etc/selinux/config or setenforce 0), which is not a good security practice, or enable an unnecessary boolean (setsebool -P httpd_can_network_connect_db on), which is not related to the issue. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 18: Securing Linux Systems, page 535.

QUESTION 4

A Linux administrator has been tasked with installing the most recent versions of packages on a RPM-based OS. Which of the following commands will accomplish this task?

A. apt-get upgrade

B. rpm -a

C. yum updateinfo

D. dnf update

E. yum check-update

Correct Answer: D

Explanation: The dnf update command will accomplish the task of installing the most recent versions of packages on a

RPM-based OS. This command will check for available updates from the enabled repositories and apply them to the

system. The apt-get upgrade command is used to install updates on a Debian-based OS, not a RPM-based OS. The rpm -a command is invalid, as -a is not a valid option for rpm. The yum updateinfo command will display information about

available updates, but it will not install them. The yum check- update command will check for available updates, but it will not install them. References: CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19:

Managing Packages and Software, page 559.

QUESTION 5

An administrator attempts to connect to a remote server by running the following command:

```
$ nmap 192.168.10.36

Starting Nmap 7.60 ( https://nmap.org ) at 2022-03-29 20:20 UTC

Nmap scan report for www1 (192.168.10.36)

Host is up (0.000091s latency).

Not shown: 979 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp filtered ssh

631/tcp open ipp

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Which of the following can be said about the remote server?

A. A firewall is blocking access to the SSH server.

B. The SSH server is not running on the remote server.

C. The remote SSH server is using SSH protocol version 1.

D. The SSH host key on the remote server has expired.

Correct Answer: A

This is because the port 22/tcp is shown as filtered by nmap, which means that nmap cannot determine whether the port is open or closed because a firewall or other device is blocking its probes. If the SSH server was not running on the remote server, the port would be shown as closed, which means that nmap received a TCP RST packet in response to its probe. If the remote SSH server was using SSH protocol version 1, the port would be shown as open, which means that nmap received a TCP SYN/ACK packet in response to its probe. If the SSH host key on the remote server had expired, the port would also be shown as open, but the SSH client would display a warning message about the host key verification failure. Therefore, the best explanation for the filtered state of the port 22/tcp is that a firewall is preventing nmap from reaching the SSH server. You can find more information about nmap port states and how to interpret them in the following web search results: Nmap scan what does STATE=filtered mean? How to find ports marked as filtered by nmap Technical Tip: NMAP scan shows ports as filtered