XK0-005 Q&As

CompTIA Linux+ Certification Exam

Pass CompTIA XK0-005 Exam with 100% Guarantee

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

https://www.pass4itsure.com/xk0-005.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

An administrator transferred a key for SSH authentication to a home directory on a remote server. The key file was moved to .ssh/authorized_keys location in order to establish SSH connection without a password. However, the SSH

command still asked for the password.

Given the following output:

```
[admin@linux ~ ]$ -ls -lhZ .ssh/auth*
-rw-r--r--. admin unconfined_u:object_r:user_home_t:s0 .ssh/authorized_keys
```

Which of the following commands would resolve the issue?

A. restorecon .ssh/authorized_keys

B. ssh_keygen -t rsa -o .ssh/authorized_keys

C. chown root:root .ssh/authorized_keys

D. chmod 600 .ssh/authorized_keys

Correct Answer: A

"restorecon" is a command in SELinux (Security-Enhanced Linux) that is used to reset the security context of a file to its default SELinux security context. The "restorecon" command can be useful in cases where the SELinux security context of a file has been altered or changed, causing issues with the file\\'s behavior or access.

The "restorecon .ssh/authorized_keys" command specifically resets the security context of the "authorized_keys" file in the ".ssh" directory to its default SELinux security context. This can be useful in cases where the SELinux security context of the "authorized_keys" file has been altered, causing issues with SSH authentication.

QUESTION 2

A Linux administrator is troubleshooting a memory-related issue. Based on the output of the commands: Which of the following commands would address the issue?

```
$ vmstat -s --unit M

968 M total memory
331 M used memory
482 M active memory
279 M inactive memory
 99 M free memory

$ free -h
              total        used        free      shared  buff/cache   available
Mem:          968M        331M         95M         13M        540M        458M
Swap:           0           0           0

$ ps -aux | grep script.sh
USER   PID   %CPU  %MEM  VSZ      RSS     TTY  STAT  START  TIME   COMMAND
user    8321 2.8   40.5  3224846  371687  7    SN    16:49  2:09   /home/user/script.sh
```

A. top -p 8321

B. kill -9 8321

C. renice -10 8321

D. free 8321

Correct Answer: B

B. kill -9 8321

If a process is causing memory issues, it may be necessary to terminate the process. The "kill" command is used to send signals to processes, and the -9 option sends the SIGKILL signal, which terminates the process immediately. By using the command "kill -9 8321", the administrator can terminate the process causing memory issues.

QUESTION 3

When trying to log in remotely to a server, a user receives the following message:

```
Password:
Last failed login: Wed Sep 15 17:23:45 CEST 2021 from 10.0.4.3 on ssh:notty
There were 3 failed login attempts since the last successful login.
Connection to localhost closed.
```

The server administrator is investigating the issue on the server and receives the following outputs:

```
Output 1:

user:x:1001:7374::/home/user:/bin/false

Output 2:

dzwx------. 2 user 62 Sep 15 17:17 /home/user

Output 3:

Sep 12 14:14:05 server sshd[22958] Failed password for user from 10.0.2.8
Sep 15 17:24:03 server sshd[8460]: Accepted keyboard-interactive/pam for user from 10.0.6.5 port 50928 ssh2
Sep 15 17:24:03 server sshd[8460]: pam_unix(sshd:session): session opened for user testuser
Sep 15 17:24:03 server sshd[8460]: pam_unix(sshd:session): session closed for user testuser
```

Which of the following is causing the issue?

A. The wrong permissions are on the user\\'s home directory.

B. The account was locked out due to three failed logins.

C. The user entered the wrong password.

D. The user has the wrong shell assigned to the account.

Correct Answer: D

QUESTION 4

A DevOps engineer needs to allow incoming traffic to ports in the range of 4000 to 5000 on a Linux server. Which of the following commands will enforce this rule?

A. iptables -f filter -I INPUT -p tcp --dport 4000:5000 -A ACCEPT

B. iptables -t filter -A INPUT -p tcp --dport 4000:5000 -j ACCEPT

C. iptables filter -A INPUT -p tcp --dport 4000:5000 -D ACCEPT

D. iptables filter -S INPUT -p tcp --dport 4000:5000 -A ACCEPT

Correct Answer: B

The command iptables is used to manage the rules in the Linux kernel\\'s firewall. The options used in the command determine how the rule will be enforced. In the case of option B, -t filter specifies that the rules should be applied to the filter table, which is used for packet filtering. The -A INPUT option specifies that the rule should be appended to the INPUT chain, which is used for incoming traffic. The -p tcp option specifies that the rule should only apply to TCP traffic, and the -dport 4000:5000 option specifies that the rule should only apply to incoming traffic to ports in the range of 4000 to 5000. The -j ACCEPT option specifies that the matching traffic should be accepted, allowing it to enter the system.

QUESTION 5

A Linux administrator modified the SSH configuration file. Which of the following commands should be used to apply the configuration changes?

A. systemctl stop sshd

B. systemctl mask sshd

C. systemctl reload sshd

D. systemctl start sshd

Correct Answer: C

The command that should be used to apply changes to the SSH configuration file is option C, systemctl reload sshd.

The reload command tells the sshd daemon to re-read its configuration file without terminating any existing connections. This makes it possible to apply changes to the SSH configuration file without disrupting any active SSH sessions.

Using the systemctl reload sshd command will cause the SSH service to reload its configuration file and apply any changes that have been made, without requiring the service to be stopped and restarted. This is the preferred method of

applying changes to the SSH configuration file because it allows changes to be made without affecting any currently connected users.

If the systemctl reload sshd command is not available, the systemctl restart sshd command can be used instead. This will stop and start the SSH service, terminating all existing connections and applying the new configuration settings.

However, this approach is less desirable because it will cause any active SSH sessions to be terminated.