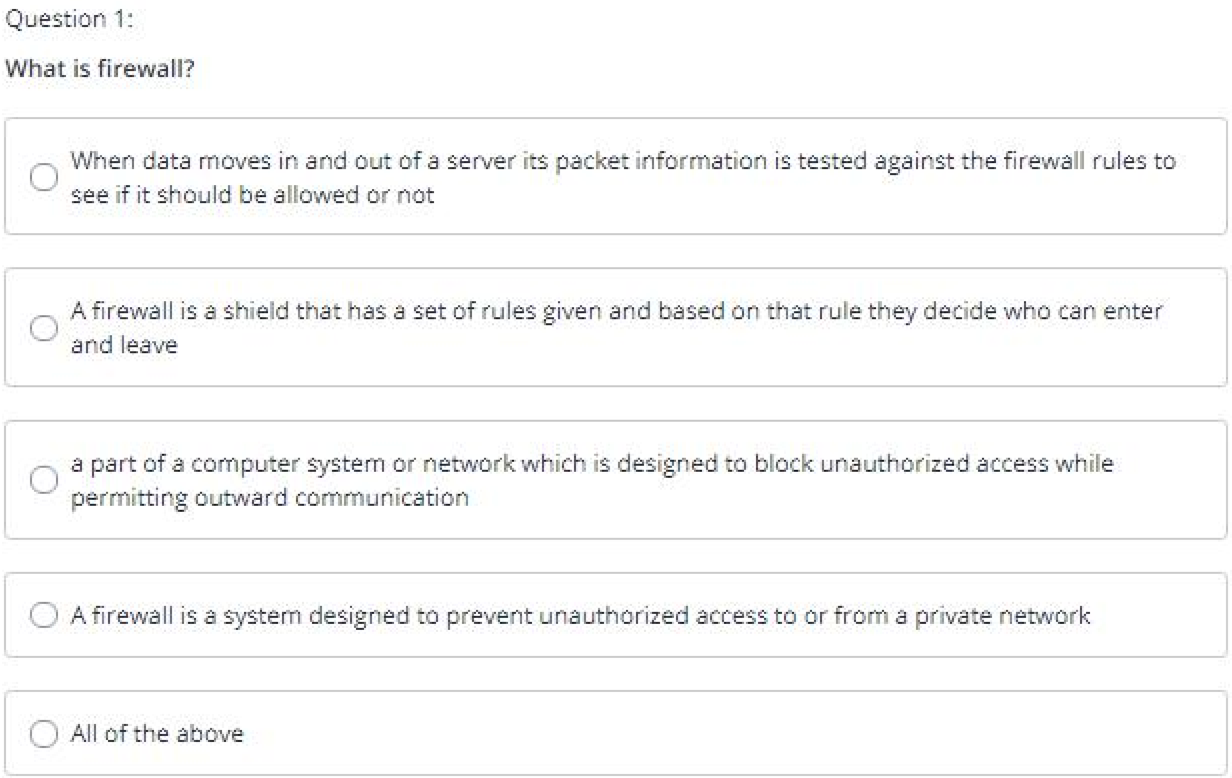
Quiz



Question 1:

What is firewall?

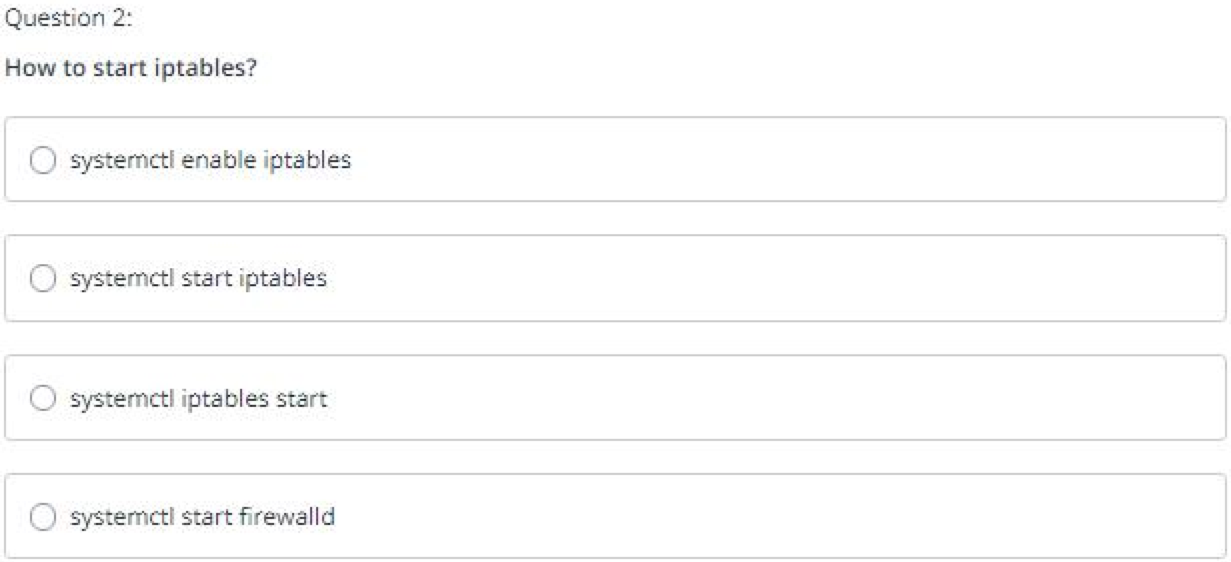
○ When data moves in and out of a server its packet information is tested against the firewall rules to see if it should be allowed or not

○ A firewall is a shield that has a set of rules given and based on that rule they decide who can enter and leave

○ a part of a computer system or network which is designed to block unauthorized access while permitting outward communication

○ A firewall is a system designed to prevent unauthorized access to or from a private network

○ All of the above



Question 2:

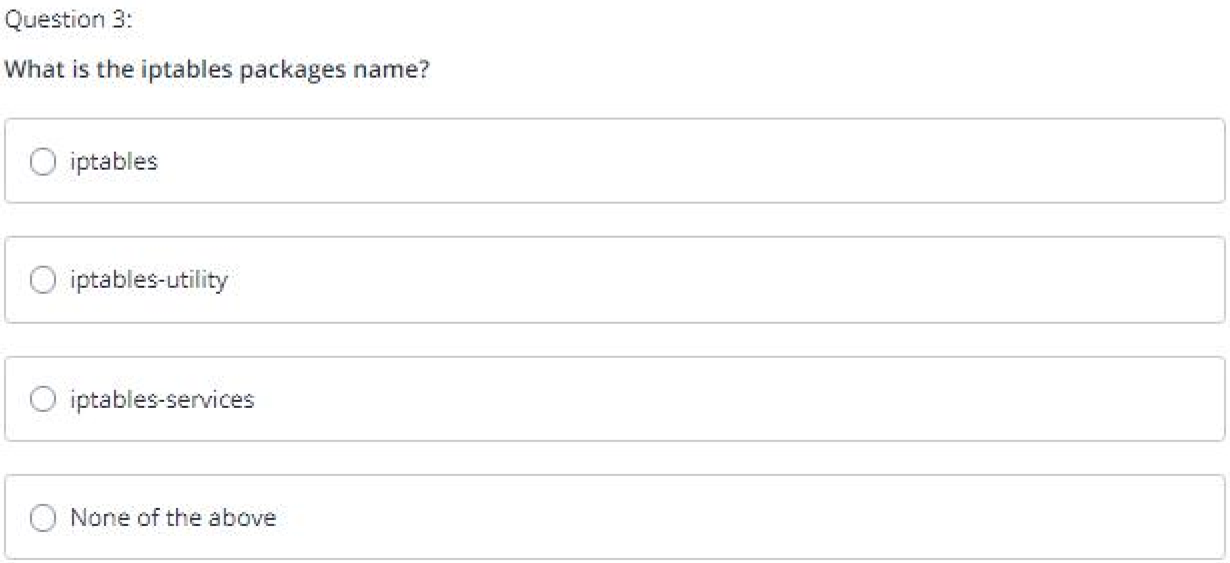
How to start iptables?

○ systemctl enable iptables

○ systemctl start iptables

○ systemctl iptables start

○ systemctl start firewalld



Question 3:

What is the iptables packages name?

○ iptables

○ iptables-utility

○ iptables-services

○ None of the above

Question 4:

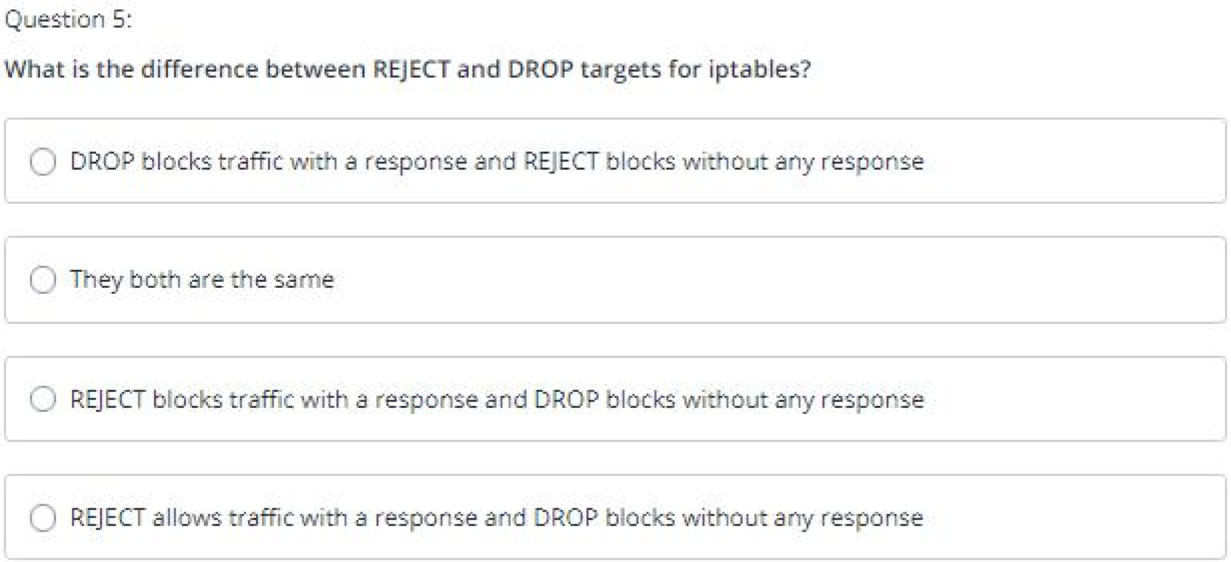
How to list iptables rules?

○ iptables -L

○ iptables -F

○ iptables -a

○ firewall-cmd --list-all



Question 5:

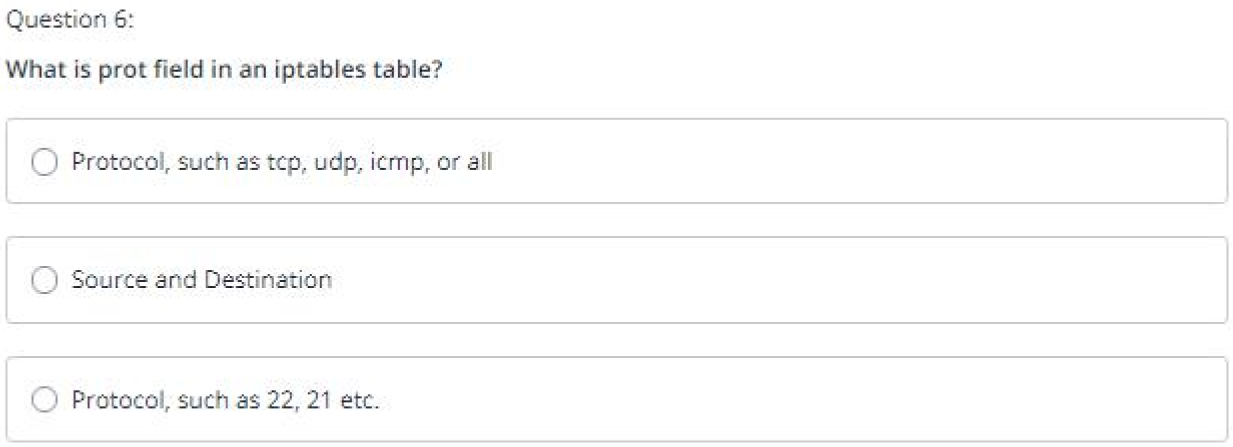
What is the difference between REJECT and DROP targets for iptables?

○ DROP blocks traffic with a response and REJECT blocks without any response

○ They both are the same

○ REJECT blocks traffic with a response and DROP blocks without any response

○ REJECT allows traffic with a response and DROP blocks without any response



Question 6:

What is prot field in an iptables table?

○ Protocol, such as tcp, udp, icmp, or all

○ Source and Destination

○ Protocol, such as 22, 21 etc.

Question 7:

Which of the following is correct?

○ Chain --> Table --> Target

○ Table --> Chain --> Target

○ Target --> Table --> Chain

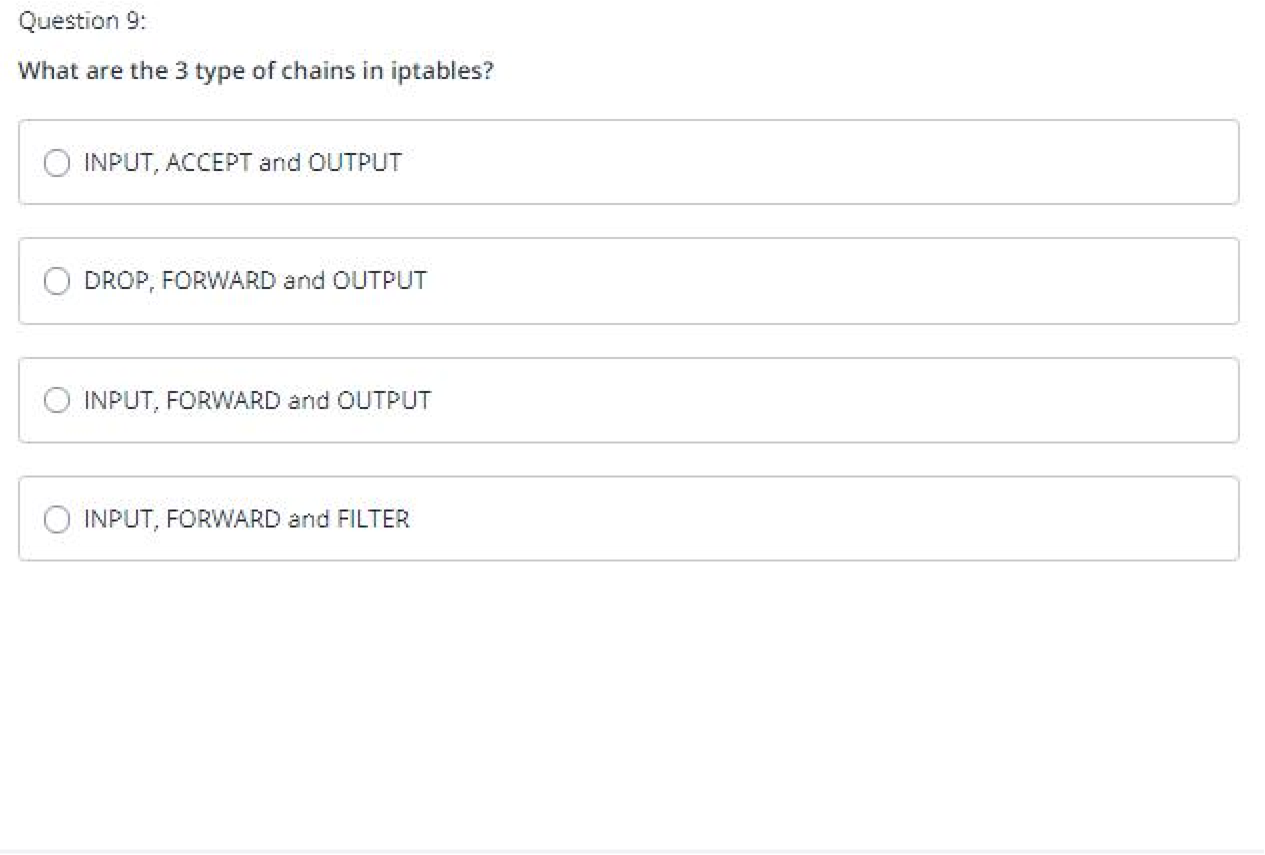
○ Chain --> Target --> Chain

Question 8:

A rule is associated with a chain

○ FALSE

○ TRUE



Question 9:

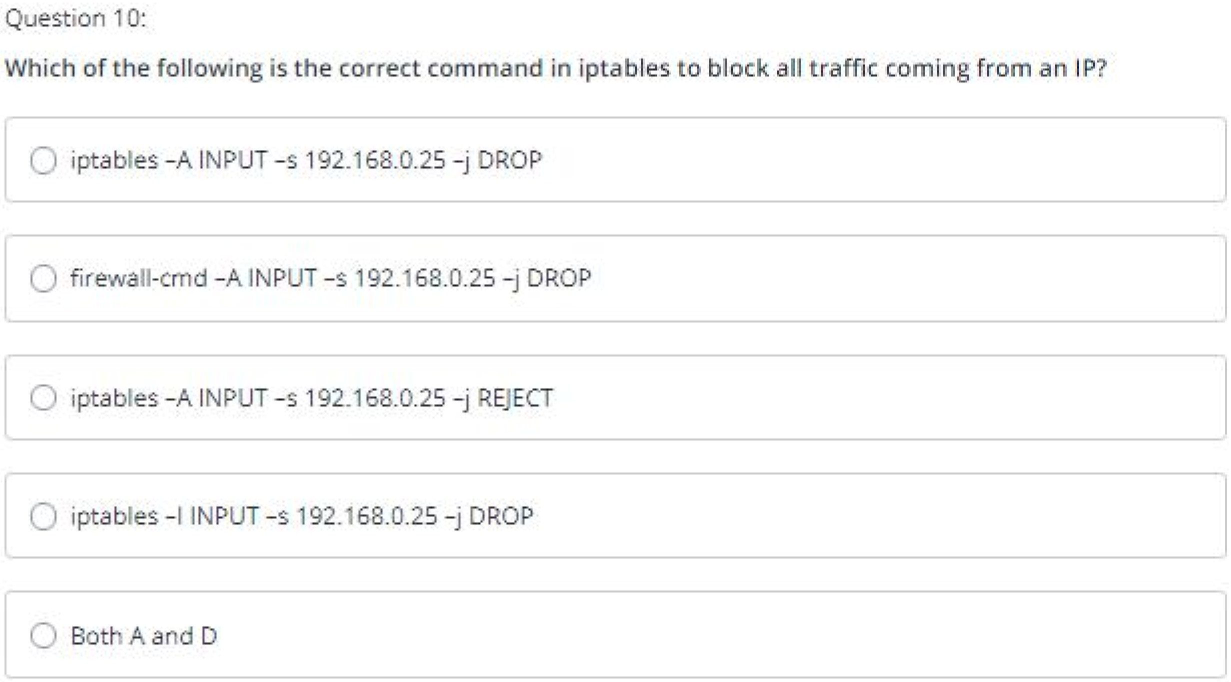
What are the 3 type of chains in iptables?

○ INPUT, ACCEPT and OUTPUT

○ DROP, FORWARD and OUTPUT

○ INPUT, FORWARD and OUTPUT

○ INPUT, FORWARD and FILTER



Question 10:

Which of the following is the correct command in iptables to block all traffic coming from an IP?

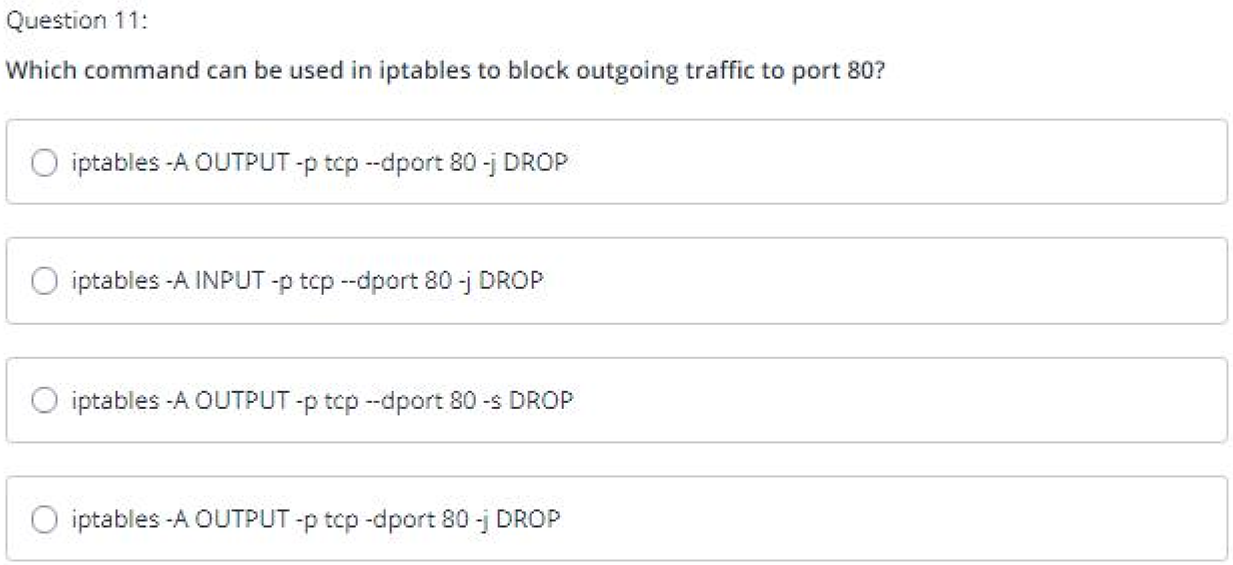
○ iptables –A INPUT –s 192.168.0.25 –j DROP

○ firewall-cmd –A INPUT –s 192.168.0.25 –j DROP

○ iptables –A INPUT –s 192.168.0.25 –j REJECT

○ iptables –I INPUT –s 192.168.0.25 –j DROP

○ Both A and D



Question 11:

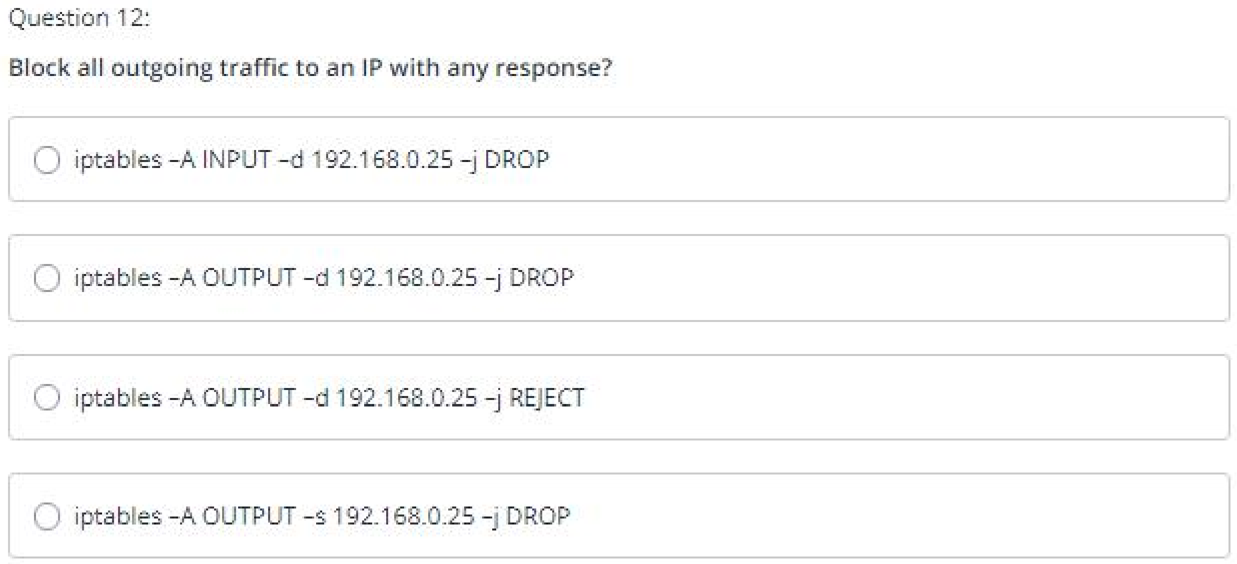
Which command can be used in iptables to block outgoing traffic to port 80?

○ iptables -A OUTPUT -p tcp --dport 80 -j DROP

○ iptables -A INPUT -p tcp --dport 80 -j DROP

○ iptables -A OUTPUT -p tcp --dport 80 -s DROP

○ iptables -A OUTPUT -p tcp -dport 80 -j DROP



Question 12:

Block all outgoing traffic to an IP with any response?

○ iptables –A INPUT –d 192.168.0.25 –j DROP

○ iptables –A OUTPUT –d 192.168.0.25 –j DROP

○ iptables –A OUTPUT –d 192.168.0.25 –j REJECT

○ iptables –A OUTPUT –s 192.168.0.25 –j DROP

Question 13:

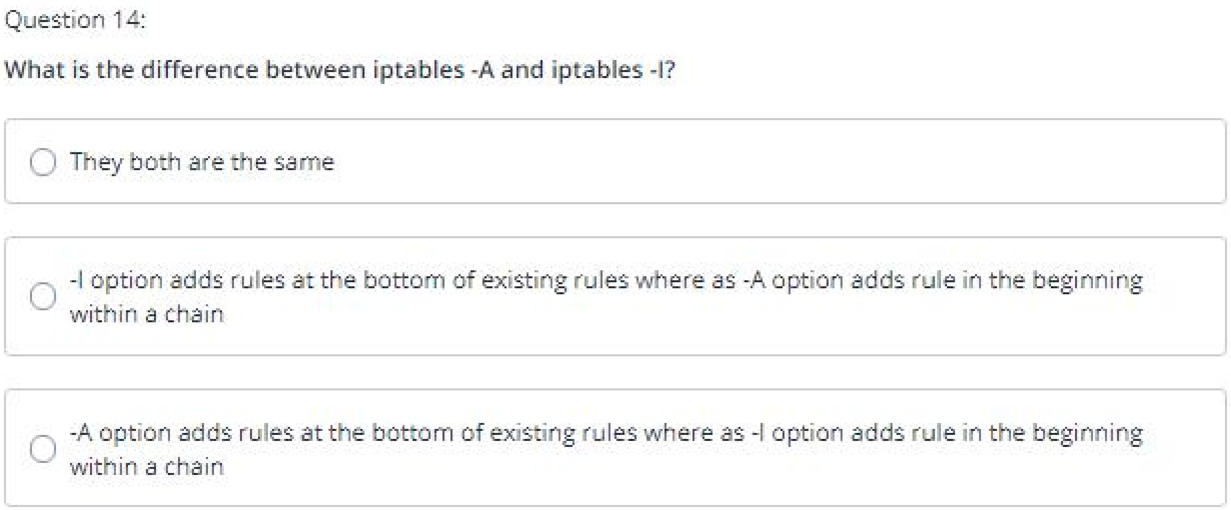
Which command is used to save the iptables?

○ iptables-allsave

○ iptable-save

○ iptables-save

○ iptables-reload



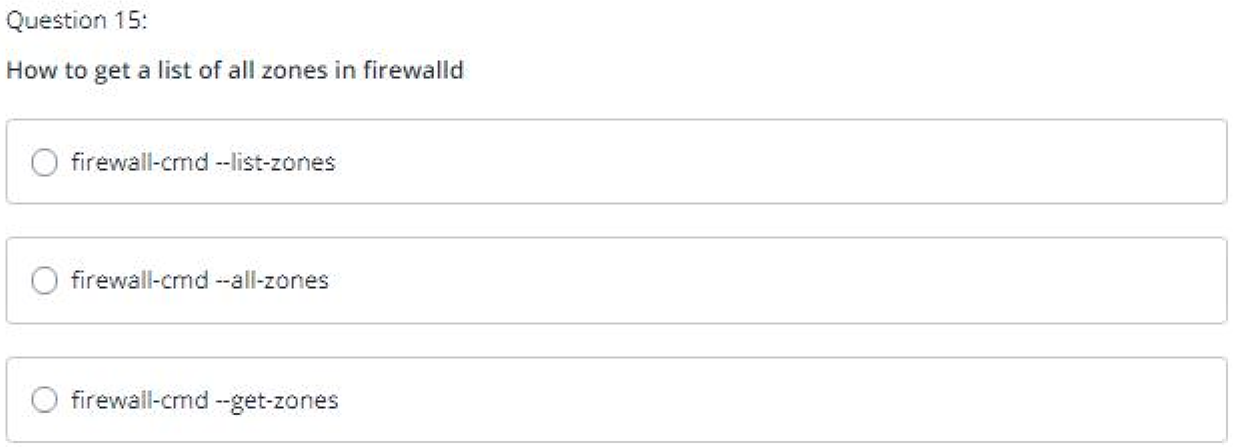
Question 14:

What is the difference between iptables -A and iptables -I?

○ They both are the same

○ -I option adds rules at the bottom of existing rules where as -A option adds rule in the beginning within a chain

○ -A option adds rules at the bottom of existing rules where as -I option adds rule in the beginning within a chain



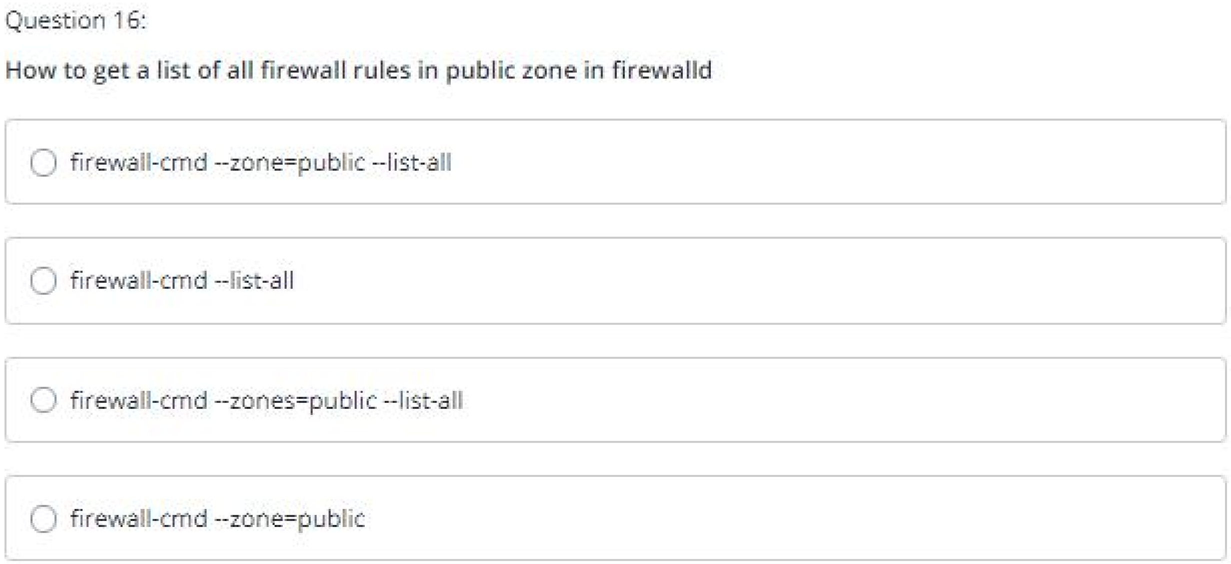
Question 15:

How to get a list of all zones in firewalld

○ firewall-cmd --list-zones

○ firewall-cmd --all-zones

○ firewall-cmd --get-zones



Question 16:

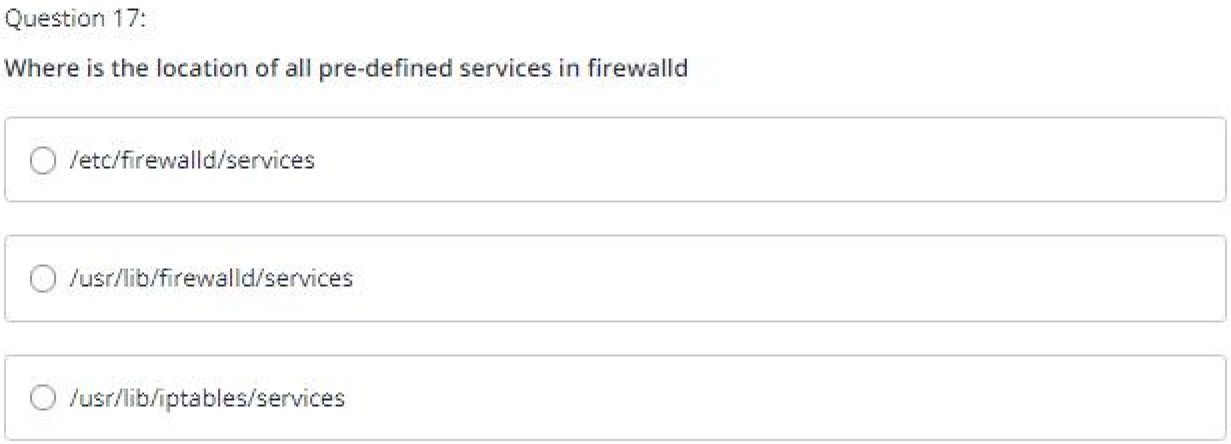
How to get a list of all firewall rules in public zone in firewalld

○ firewall-cmd --zone=public --list-all

○ firewall-cmd --list-all

○ firewall-cmd --zones=public --list-all

○ firewall-cmd --zone=public



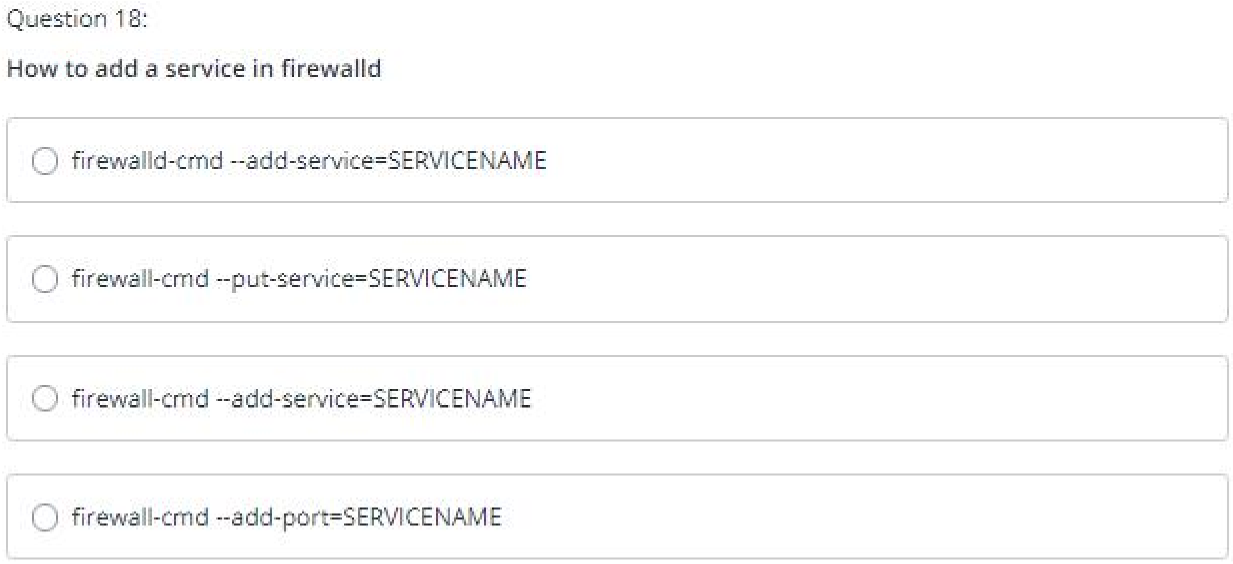
Question 17:

Where is the location of all pre-defined services in firewalld

○ /etc/firewalld/services

○ /usr/lib/firewalld/services

○ /usr/lib/iptables/services



Question 18:

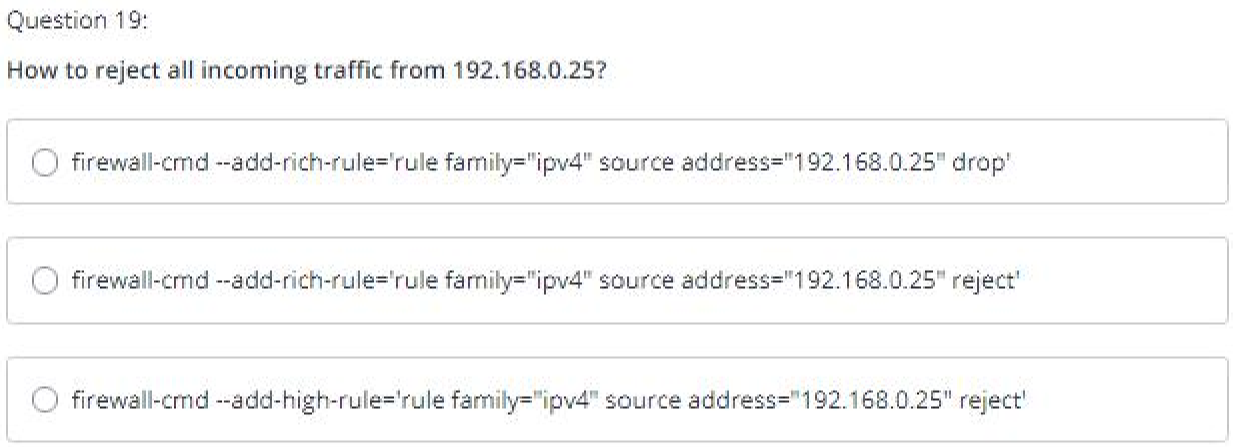
How to add a service in firewalld

○ firewalld-cmd --add-service=SERVICENAME

○ firewall-cmd --put-service=SERVICENAME

○ firewall-cmd --add-service=SERVICENAME

○ firewall-cmd --add-port=SERVICENAME



Question 19:

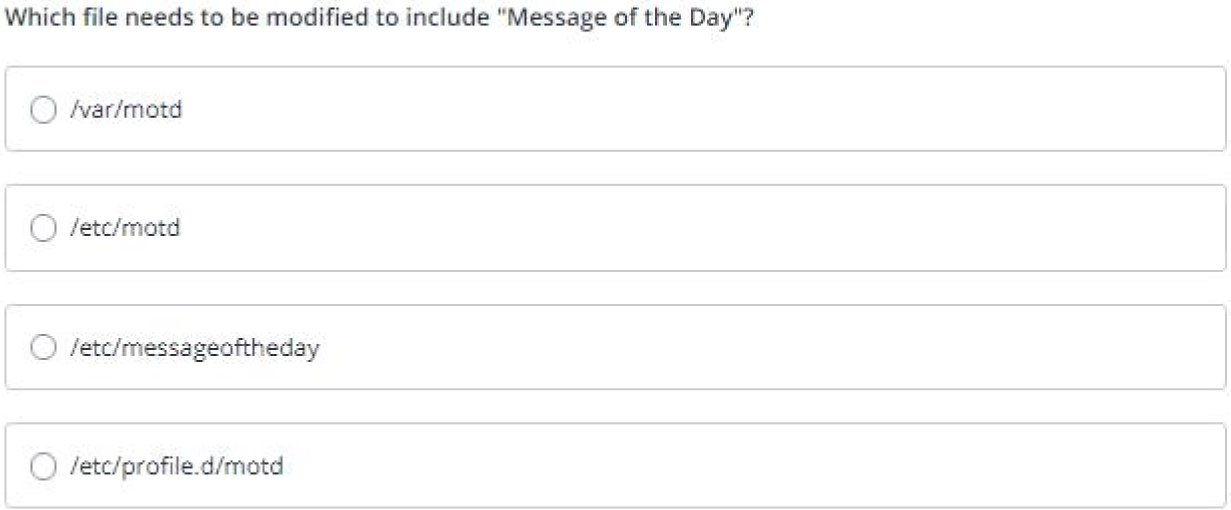
How to reject all incoming traffic from 192.168.0.25?

○ firewall-cmd --add-rich-rule='rule family="ipv4" source address="192.168.0.25" drop'

○ firewall-cmd --add-rich-rule='rule family="ipv4" source address="192.168.0.25" reject'

○ firewall-cmd --add-high-rule='rule family="ipv4" source address="192.168.0.25" reject'

20



Which file needs to be modified to include "Message of the Day"?

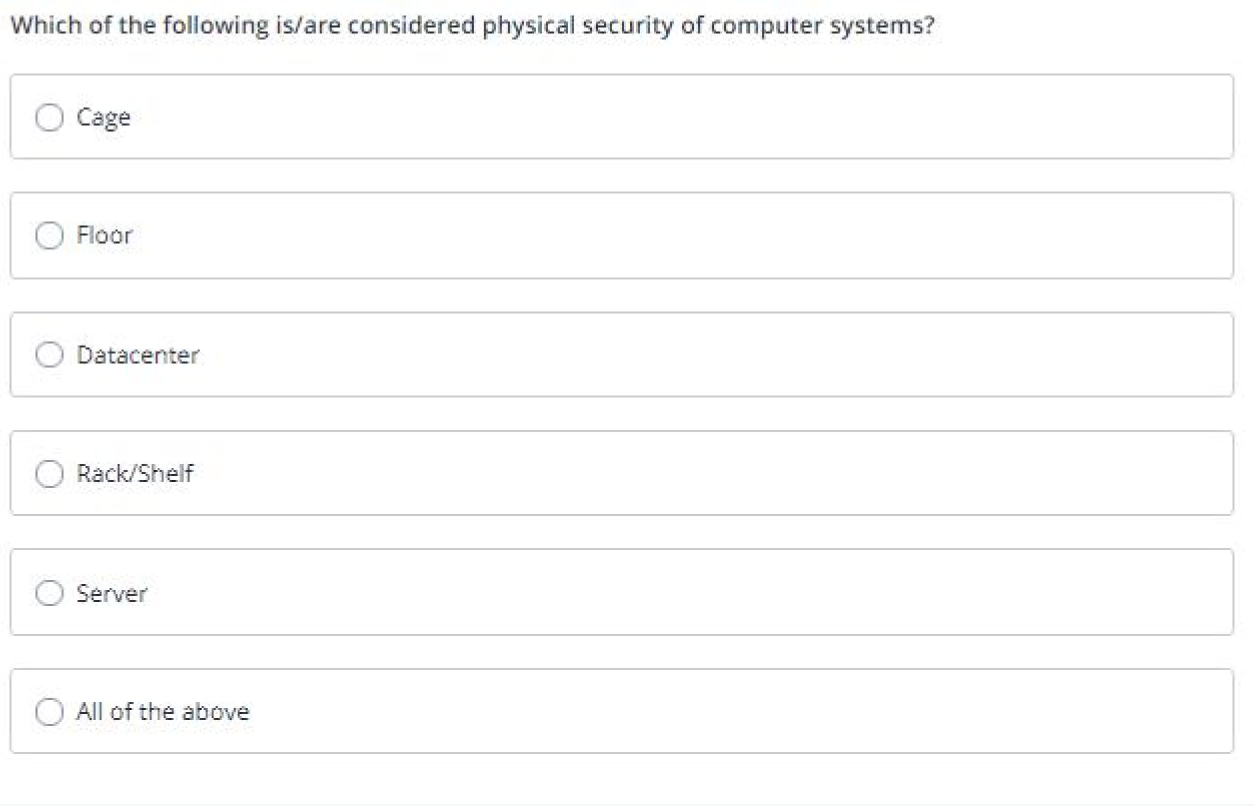
○ /var/motd

○ /etc/motd

○ /etc/messageoftheday

○ /etc/profile.d/motd

21



Which of the following is/are considered physical security of computer systems?

○ Cage

○ Floor

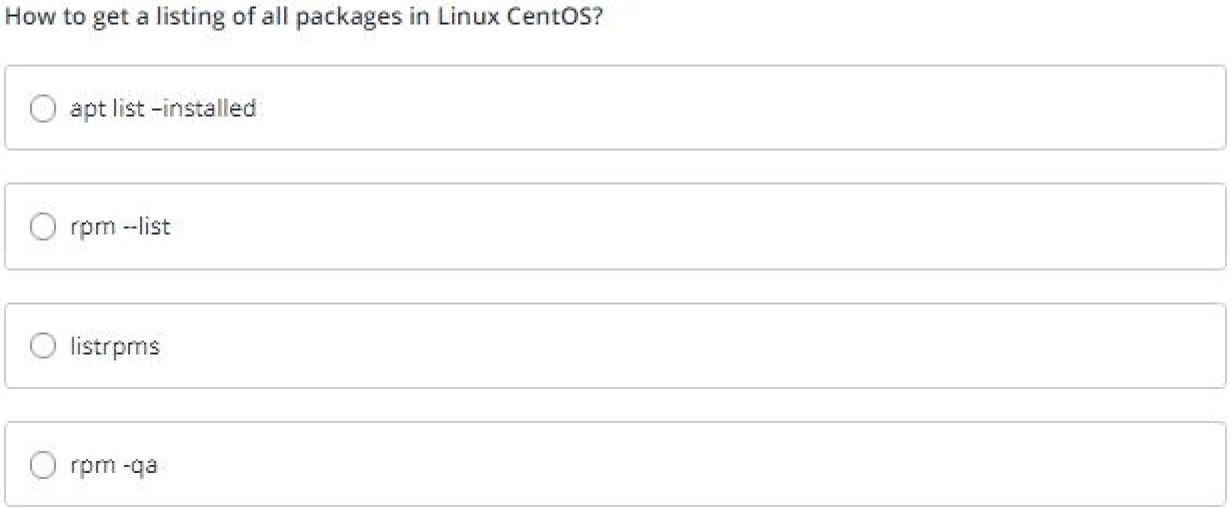
○ Datacenter

○ Rack/Shelf

○ Server

○ All of the above

22



How to get a listing of all packages in Linux CentOS?

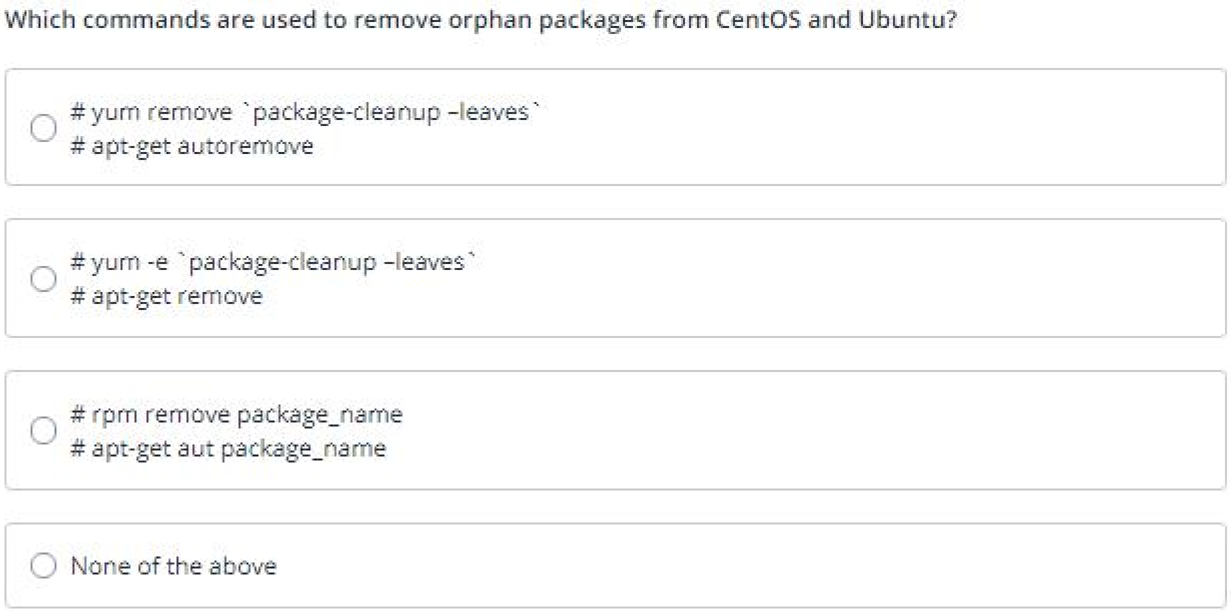
○ apt list –installed

○ rpm --list

○ listrpms

○ rpm -qa

23



Which commands are used to remove orphan packages from CentOS and Ubuntu?

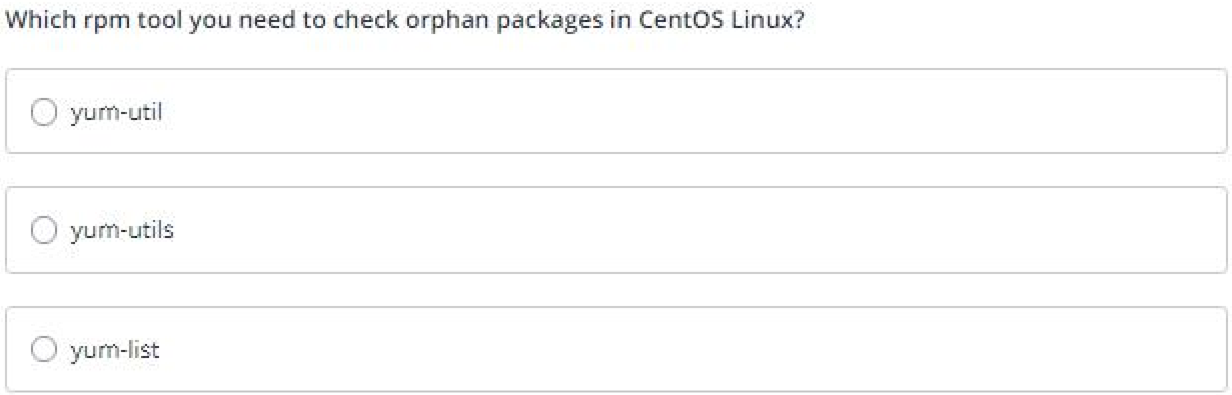
○
```
# yum remove `package-cleanup –leaves`
# apt-get autoremove
```

○
```
# yum -e `package-cleanup –leaves`
# apt-get remove
```

○
```
# rpm remove package_name
# apt-get aut package_name
```

○ None of the above

24



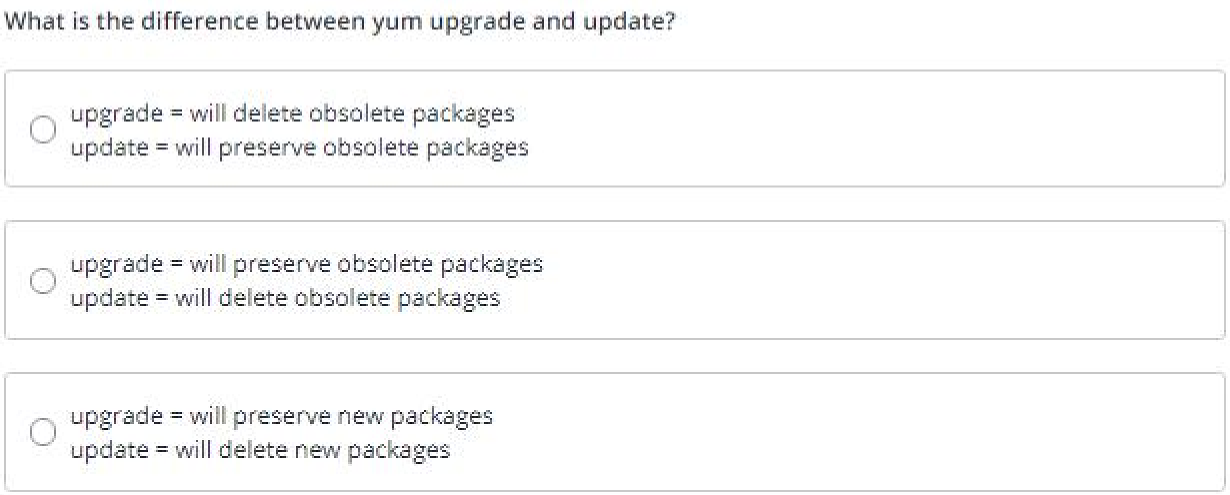
Which rpm tool you need to check orphan packages in CentOS Linux?

○ yum-util

○ yum-utils

○ yum-list

25



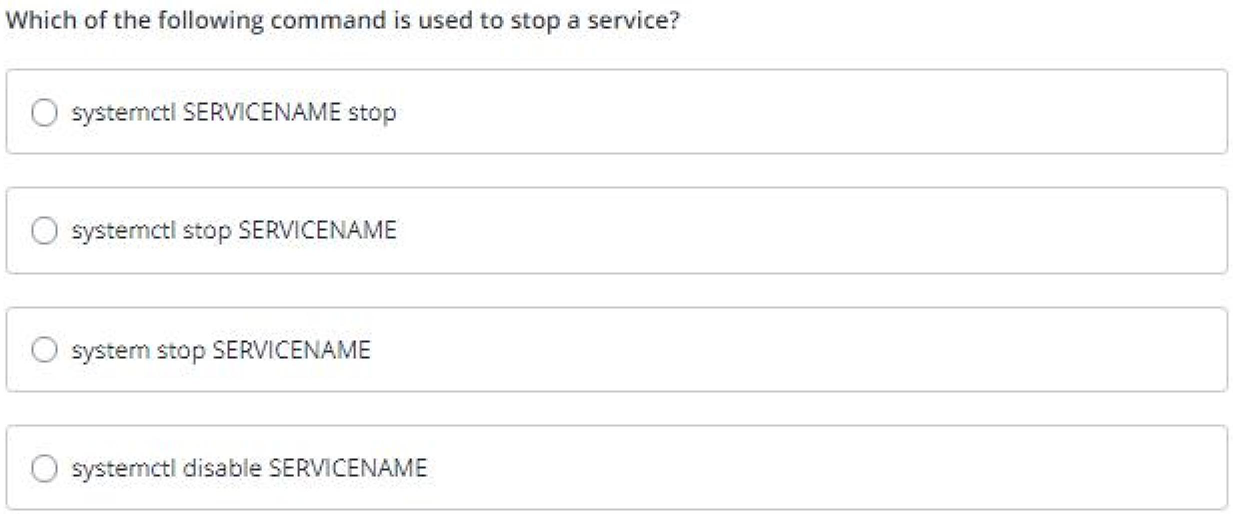
What is the difference between yum upgrade and update?

○ upgrade = will delete obsolete packages
update = will preserve obsolete packages

○ upgrade = will preserve obsolete packages
update = will delete obsolete packages

○ upgrade = will preserve new packages
update = will delete new packages

26



Which of the following command is used to stop a service?

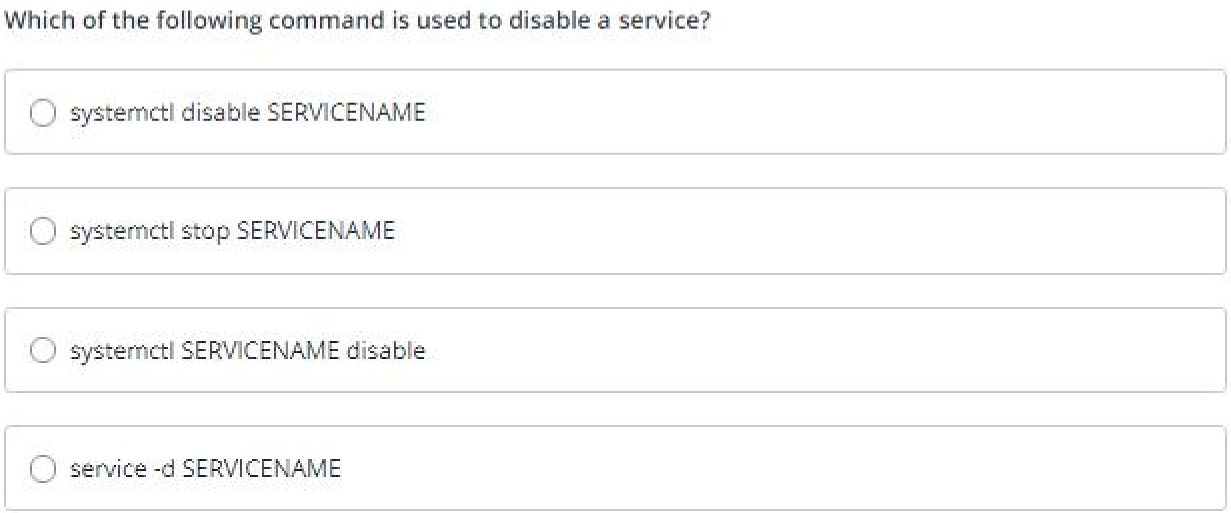
○ systemctl SERVICENAME stop

○ systemctl stop SERVICENAME

○ system stop SERVICENAME

○ systemctl disable SERVICENAME

27



Which of the following command is used to disable a service?

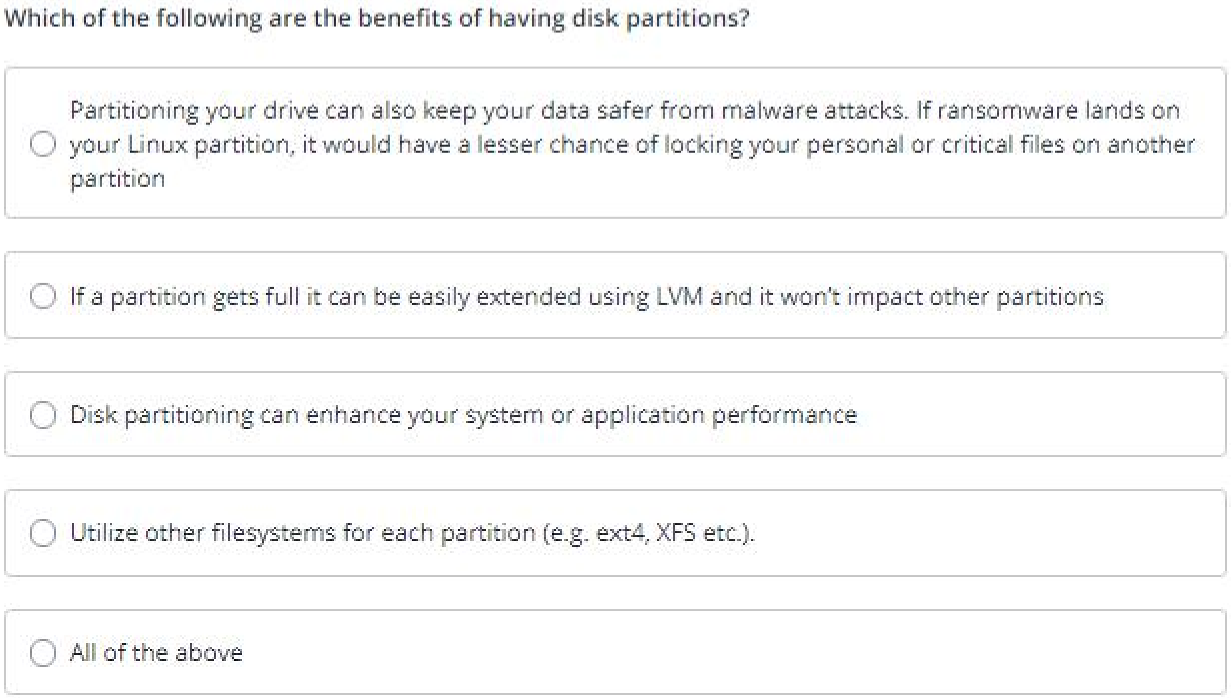
○ systemctl disable SERVICENAME

○ systemctl stop SERVICENAME

○ systemctl SERVICENAME disable

○ service -d SERVICENAME

28



Which of the following are the benefits of having disk partitions?

○ Partitioning your drive can also keep your data safer from malware attacks. If ransomware lands on your Linux partition, it would have a lesser chance of locking your personal or critical files on another partition

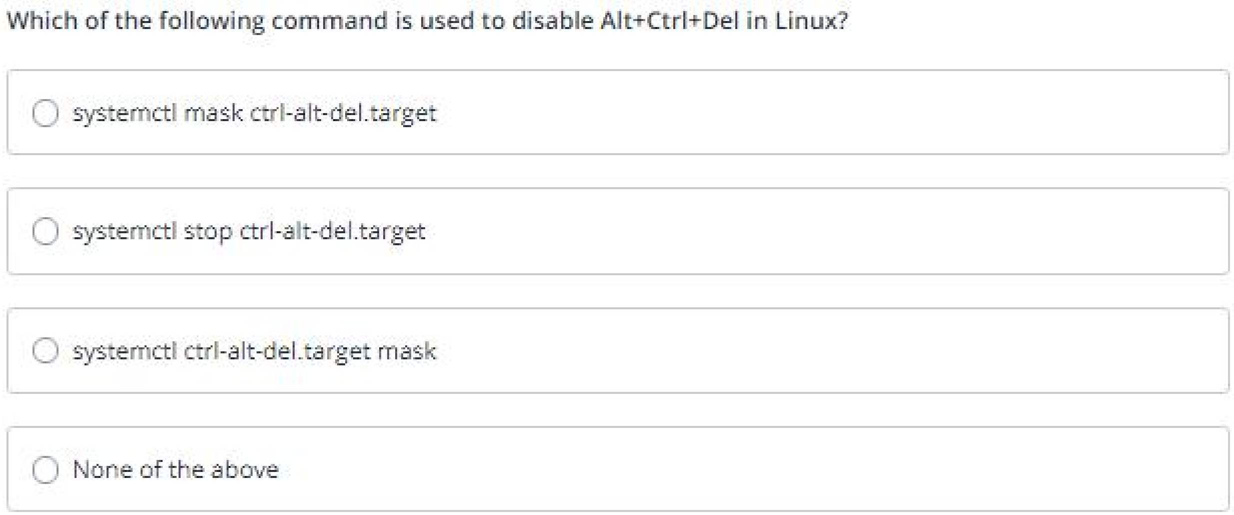
○ If a partition gets full it can be easily extended using LVM and it won't impact other partitions

○ Disk partitioning can enhance your system or application performance

○ Utilize other filesystems for each partition (e.g. ext4, XFS etc.).

○ All of the above

29



Which of the following command is used to disable Alt+Ctrl+Del in Linux?

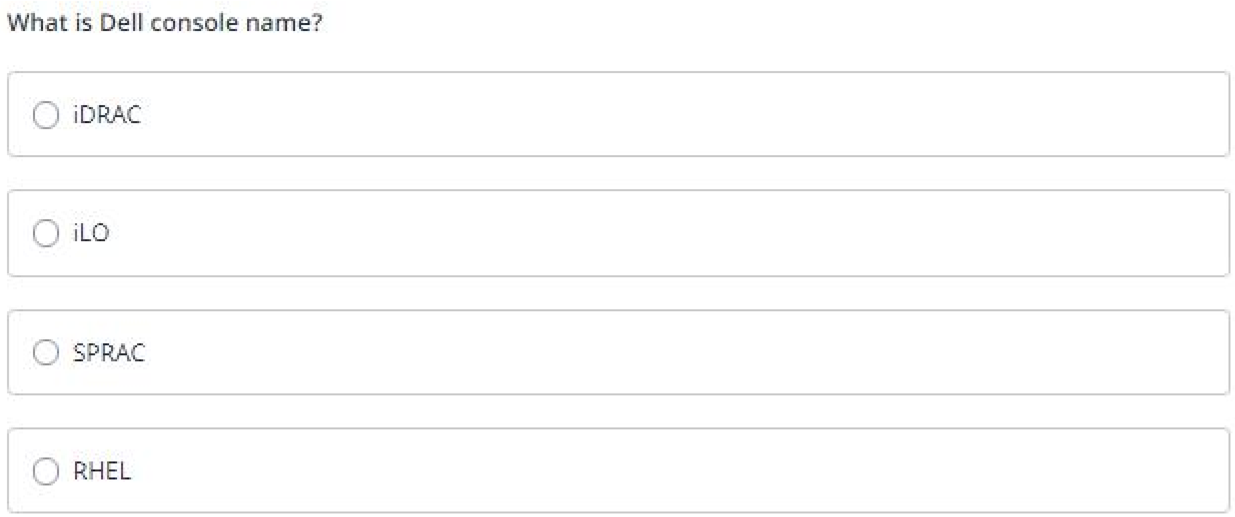
○ systemctl mask ctrl-alt-del.target

○ systemctl stop ctrl-alt-del.target

○ systemctl ctrl-alt-del.target mask

○ None of the above

30



What is Dell console name?

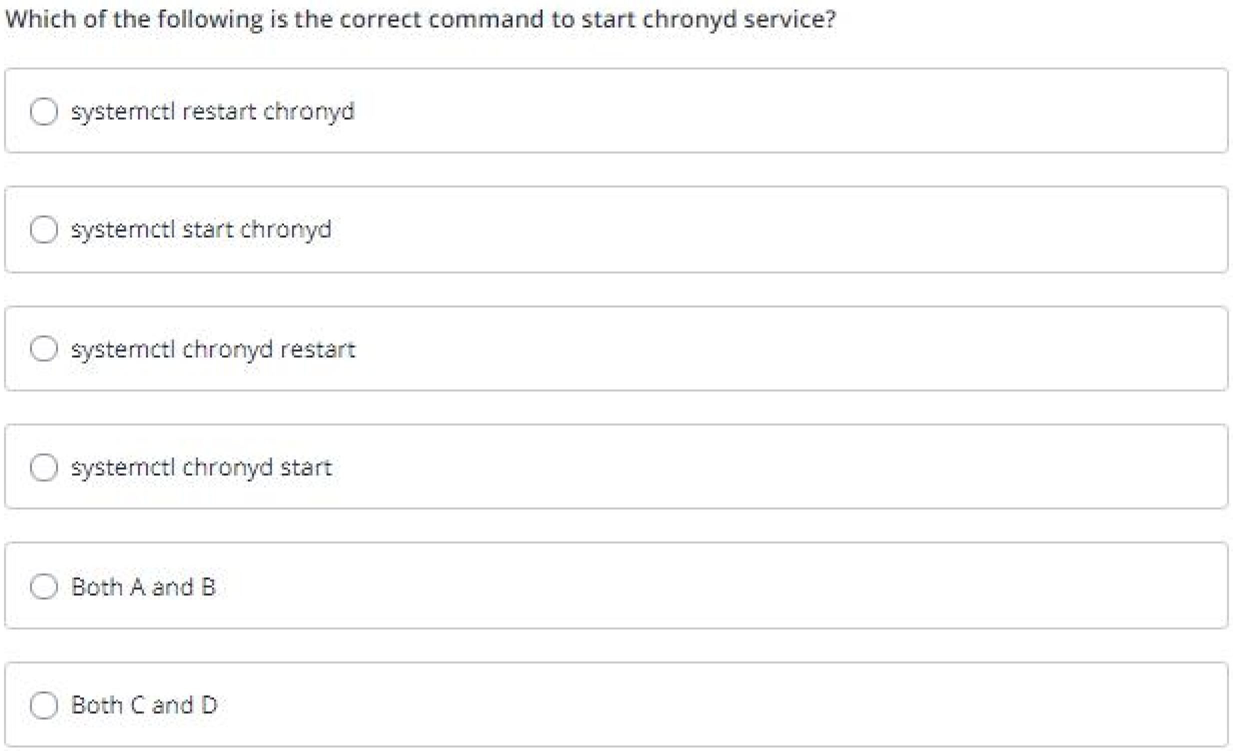
○ iDRAC

○ iLO

○ SPRAC

○ RHEL

31



Which of the following is the correct command to start chronyd service?

○ systemctl restart chronyd

○ systemctl start chronyd

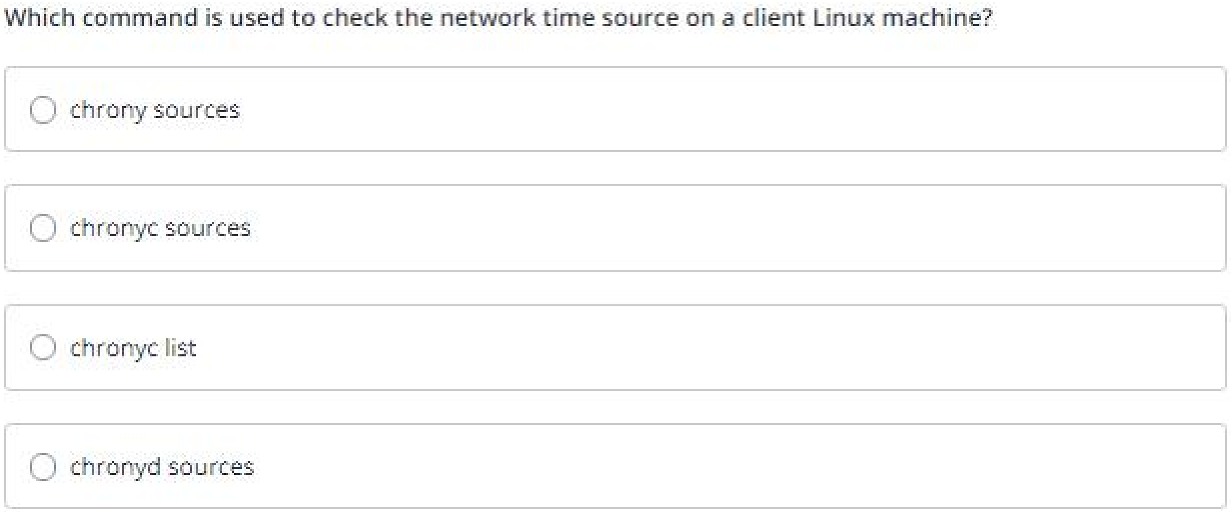
○ systemctl chronyd restart

○ systemctl chronyd start

○ Both A and B

○ Both C and D

32



Which command is used to check the network time source on a client Linux machine?

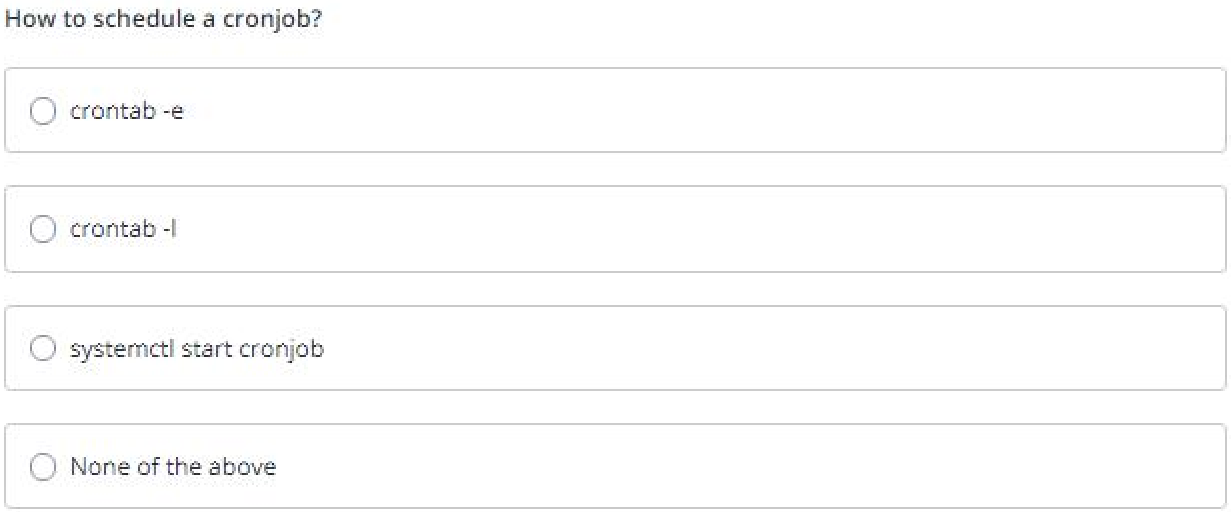
○ chrony sources

○ chronyc sources

○ chronyc list

○ chronyd sources

33



How to schedule a cronjob?

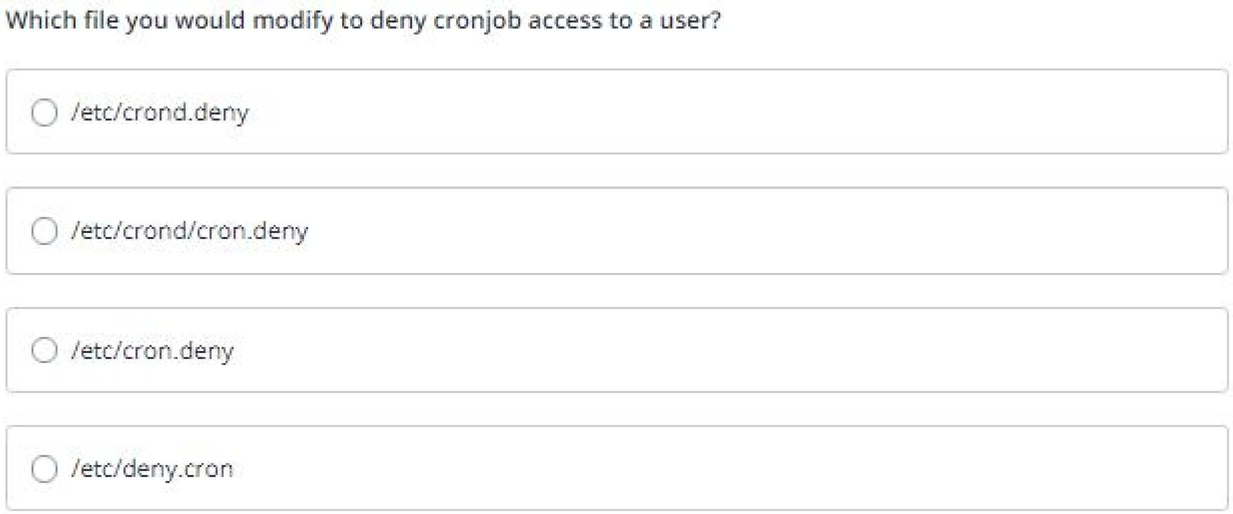
○ crontab -e

○ crontab -l

○ systemctl start cronjob

○ None of the above

34



Which file you would modify to deny cronjob access to a user?

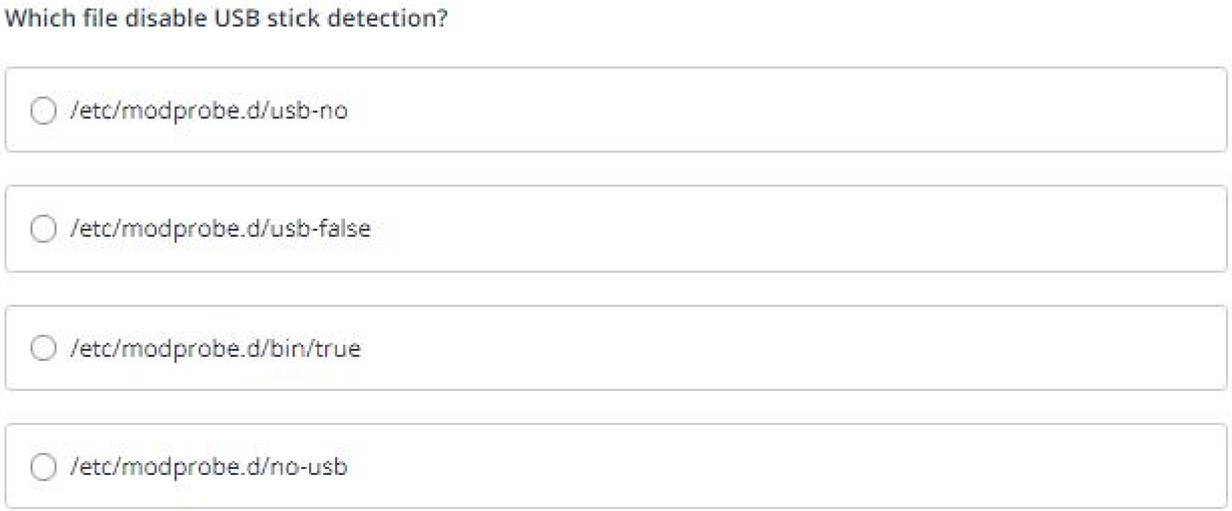
○ /etc/crond.deny

○ /etc/crond/cron.deny

○ /etc/cron.deny

○ /etc/deny.cron

35



Which file disable USB stick detection?

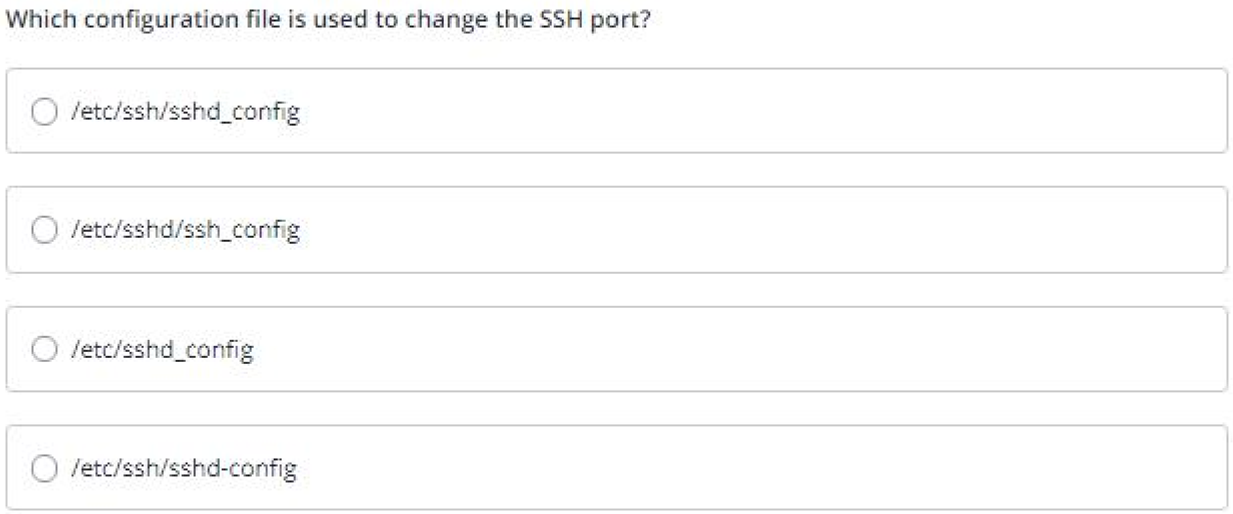
○ /etc/modprobe.d/usb-no

○ /etc/modprobe.d/usb-false

○ /etc/modprobe.d/bin/true

○ /etc/modprobe.d/no-usb

36



Which configuration file is used to change the SSH port?

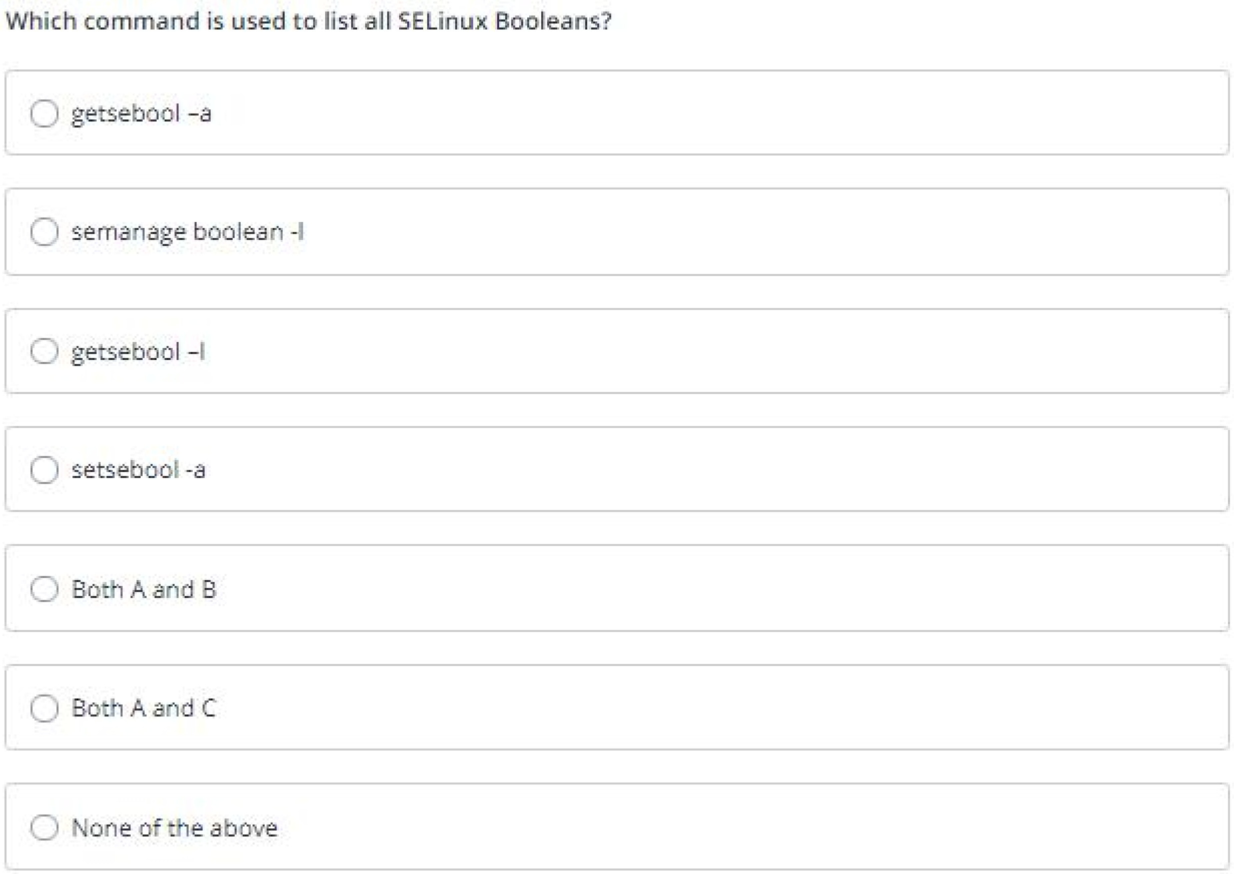
○ /etc/ssh/sshd_config

○ /etc/sshd/ssh_config

○ /etc/sshd_config

○ /etc/ssh/sshd-config

37



Which command is used to list all SELinux Booleans?

○ getsebool –a

○ semanage boolean -l

○ getsebool –l

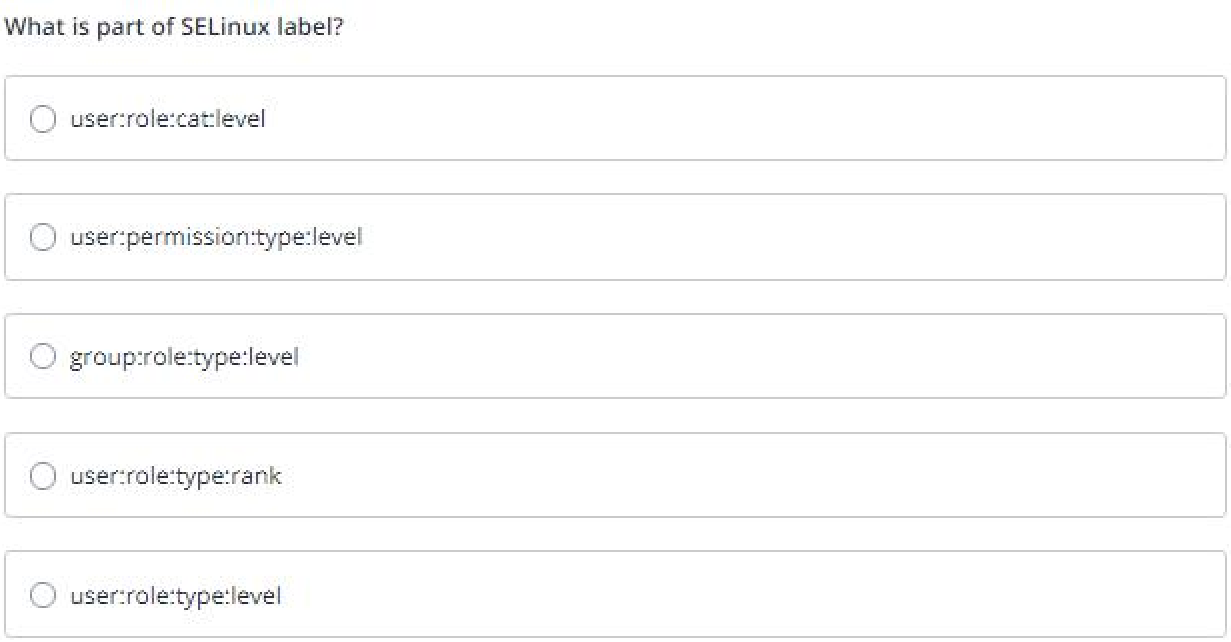
○ setsebool -a

○ Both A and B

○ Both A and C

○ None of the above

38



What is part of SELinux label?

○ user:role:cat:level

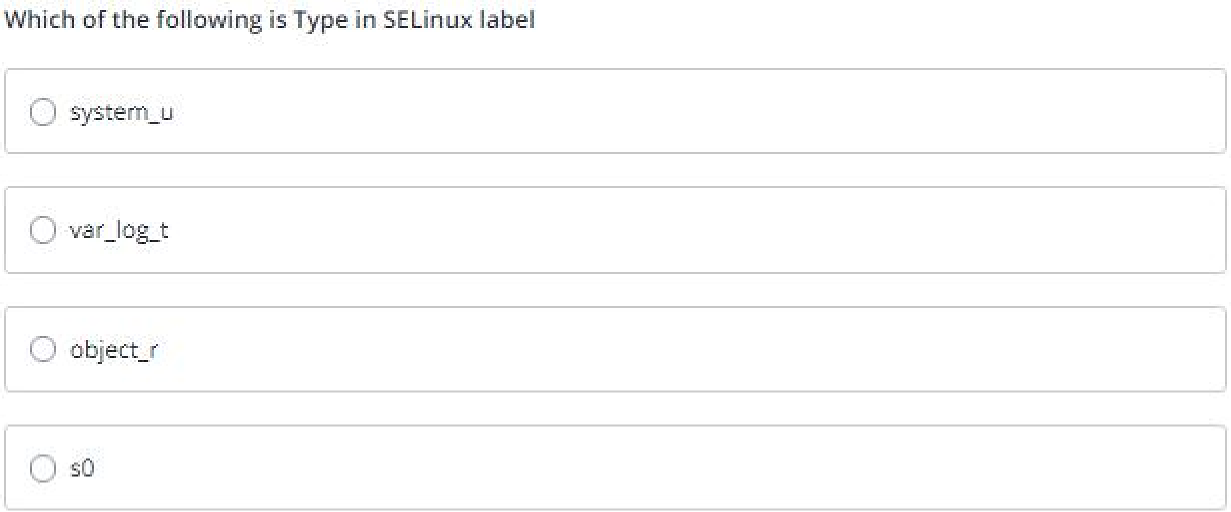
○ user:permission:type:level

○ group:role:type:level

○ user:role:type:rank

○ user:role:type:level

39



Which of the following is Type in SELinux label

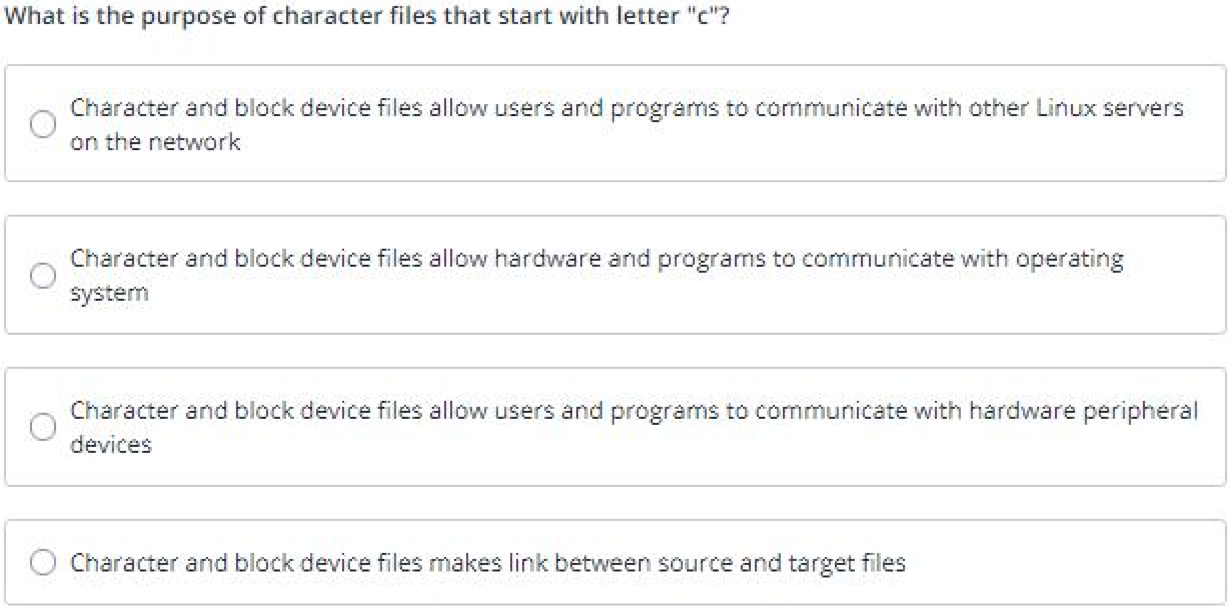
○ system_u

○ var_log_t

○ object_r

○ s0

40



What is the purpose of character files that start with letter "c"?

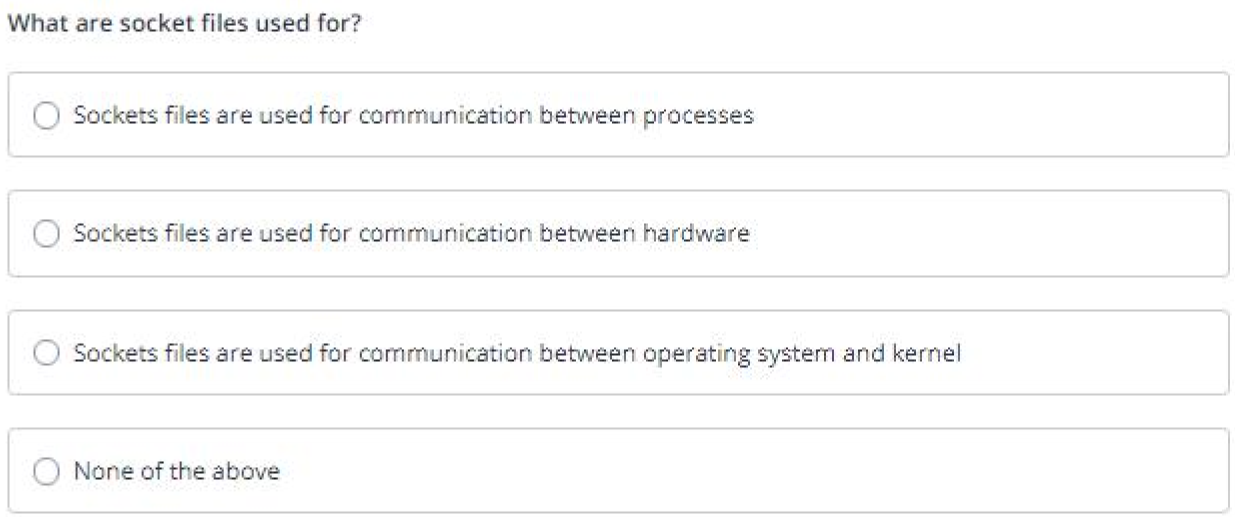
○ Character and block device files allow users and programs to communicate with other Linux servers on the network

○ Character and block device files allow hardware and programs to communicate with operating system

○ Character and block device files allow users and programs to communicate with hardware peripheral devices

○ Character and block device files makes link between source and target files

41



What are socket files used for?

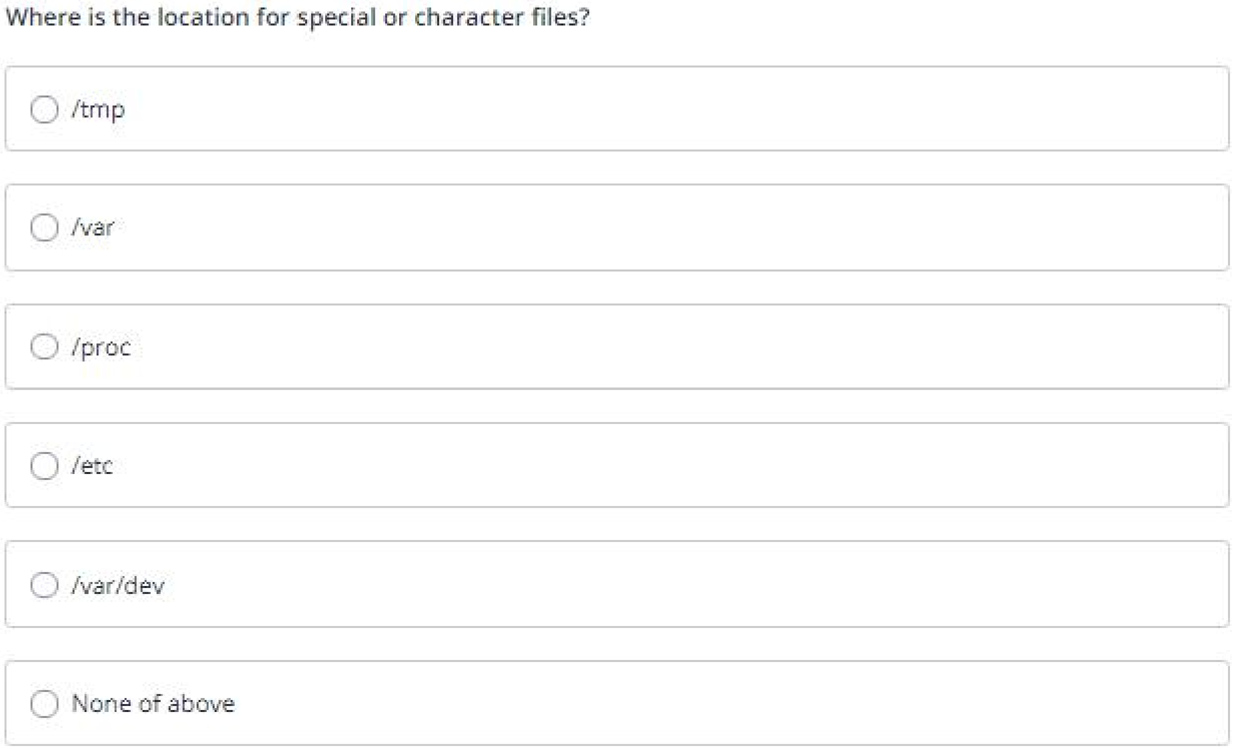
○ Sockets files are used for communication between processes

○ Sockets files are used for communication between hardware

○ Sockets files are used for communication between operating system and kernel

○ None of the above

42



Where is the location for special or character files?

○ /tmp

○ /var

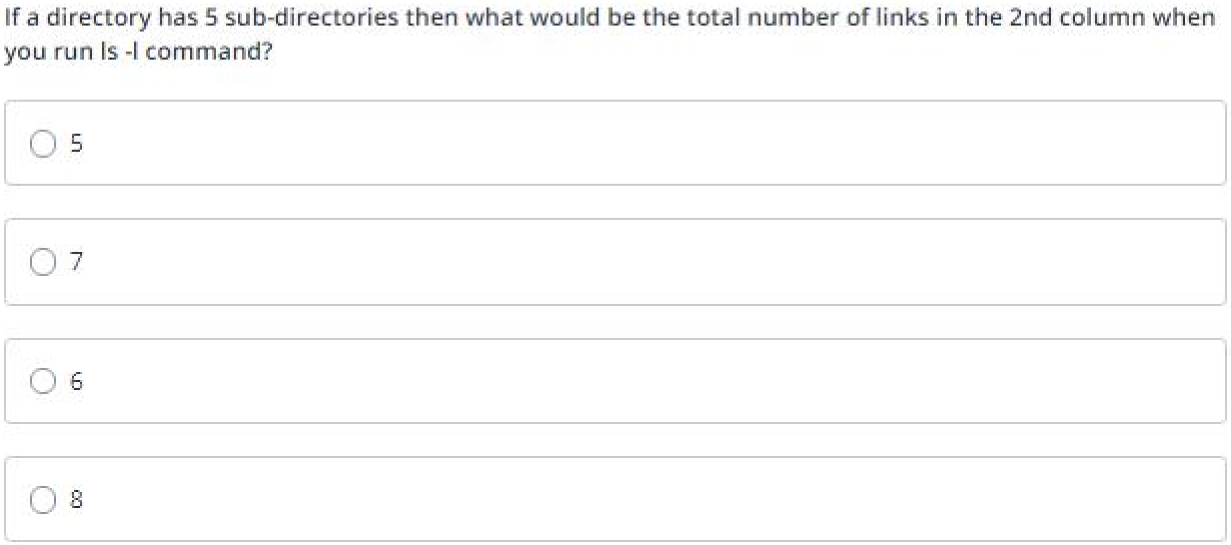
○ /proc

○ /etc

○ /var/dev

○ None of above

43



If a directory has 5 sub-directories then what would be the total number of links in the 2nd column when you run ls -l command?

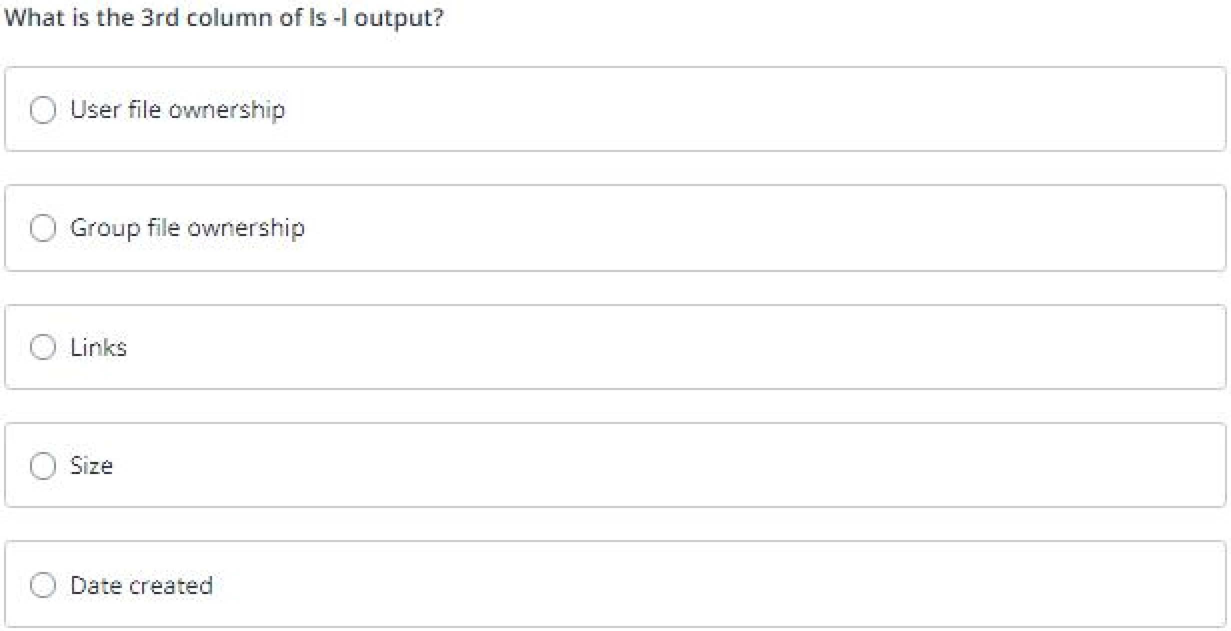
○ 5

○ 7

○ 6

○ 8

44



What is the 3rd column of ls -l output?

○ User file ownership

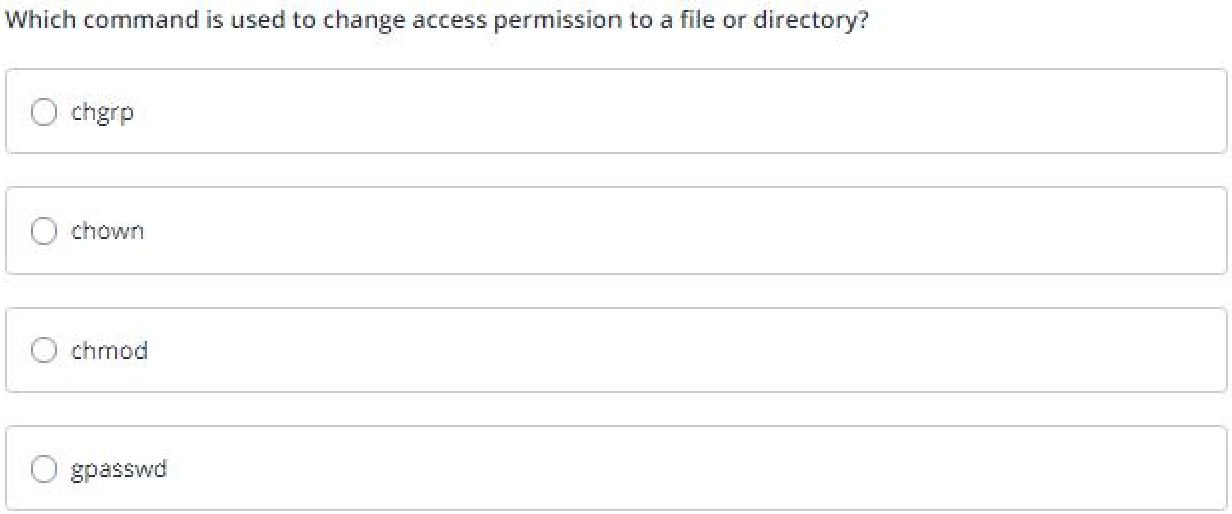
○ Group file ownership

○ Links

○ Size

○ Date created

45



Which command is used to change access permission to a file or directory?

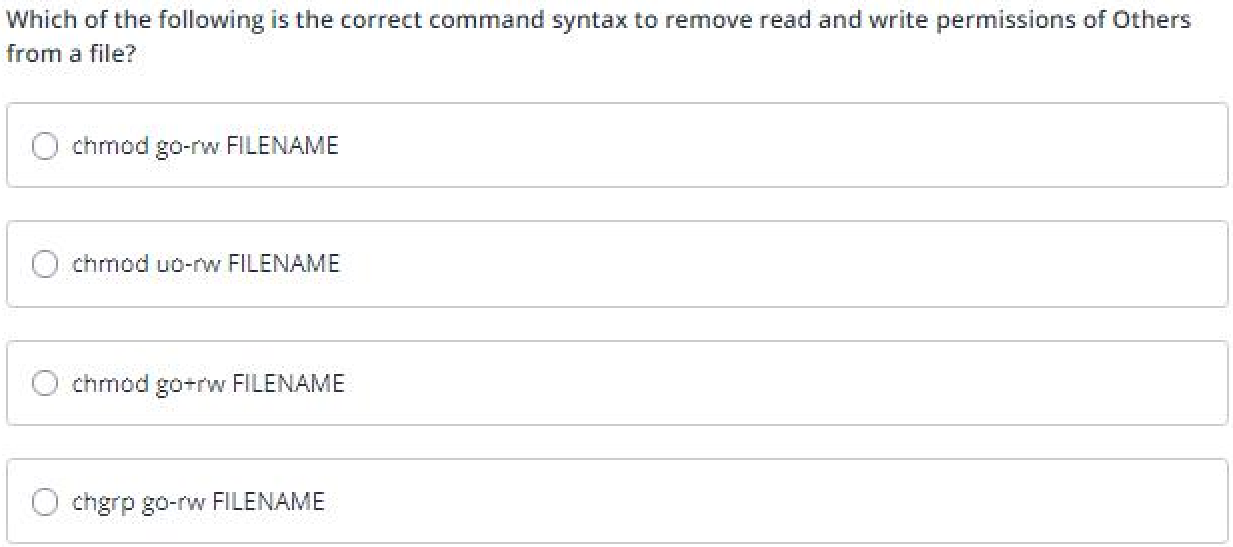
○ chgrp

○ chown

○ chmod

○ gpasswd

46



Which of the following is the correct command syntax to remove read and write permissions of Others from a file?

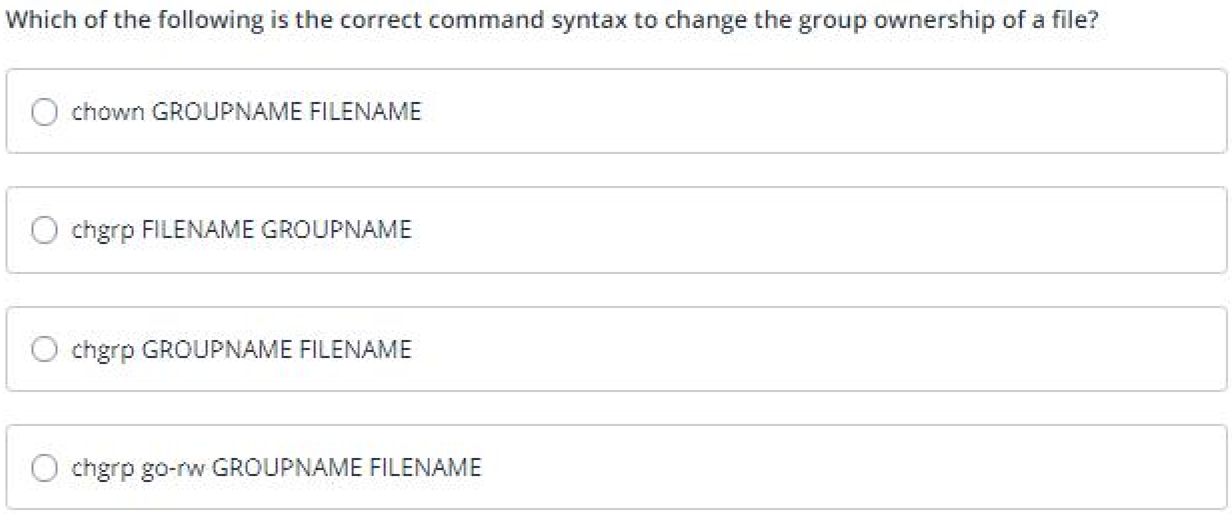
○ chmod go-rw FILENAME

○ chmod uo-rw FILENAME

○ chmod go+rw FILENAME

○ chgrp go-rw FILENAME

47



Which of the following is the correct command syntax to change the group ownership of a file?

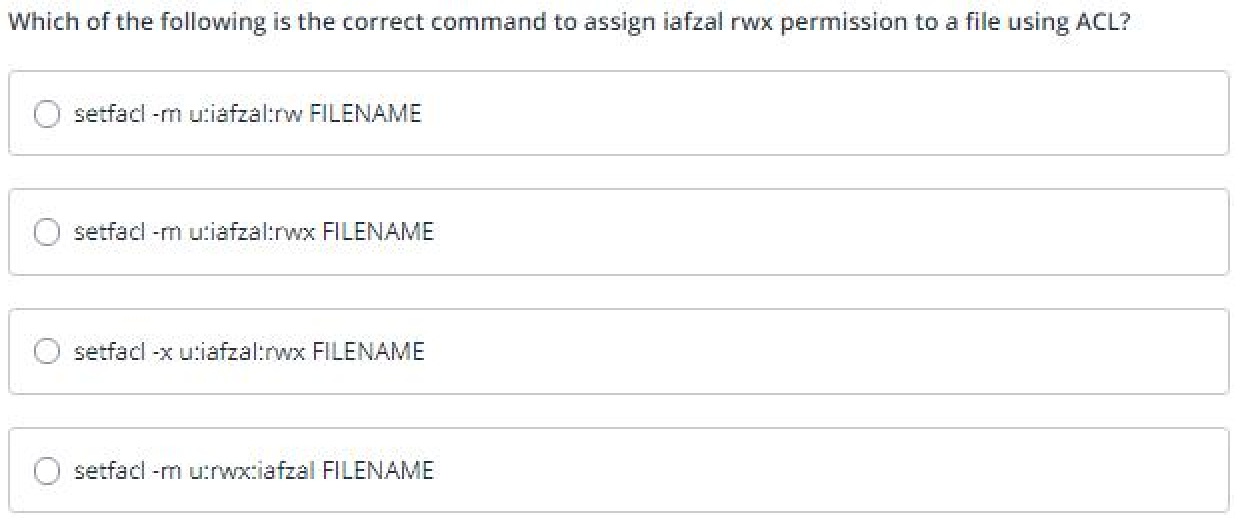
○ chown GROUPNAME FILENAME

○ chgrp FILENAME GROUPNAME

○ chgrp GROUPNAME FILENAME

○ chgrp go-rw GROUPNAME FILENAME

48



Which of the following is the correct command to assign iafzal rwx permission to a file using ACL?

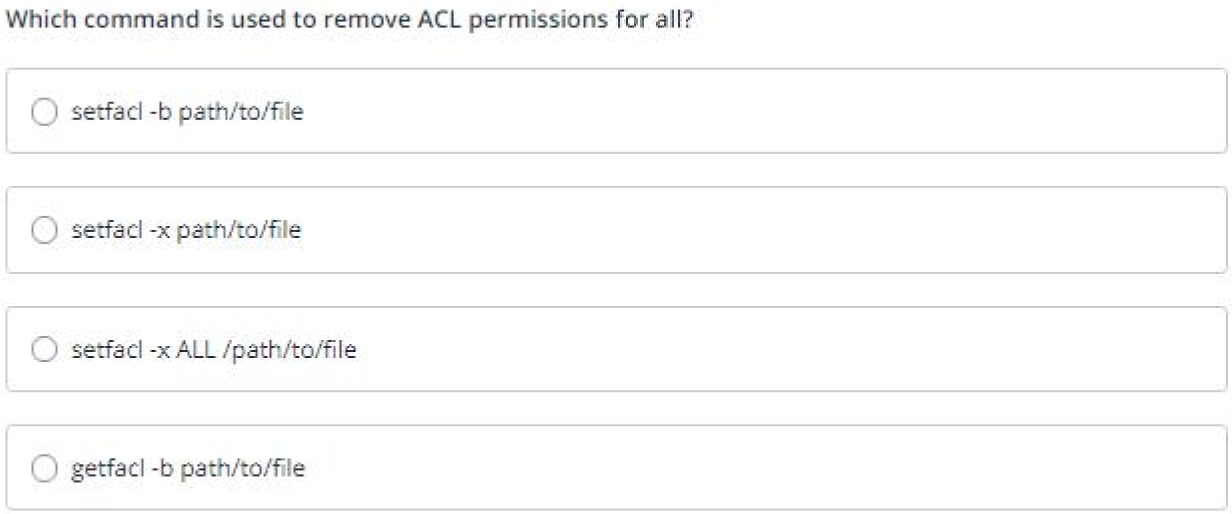
○ setfacl -m u:iafzal:rw FILENAME

○ setfacl -m u:iafzal:rwx FILENAME

○ setfacl -x u:iafzal:rwx FILENAME

○ setfacl -m u:rwx:iafzal FILENAME

49



Which command is used to remove ACL permissions for all?

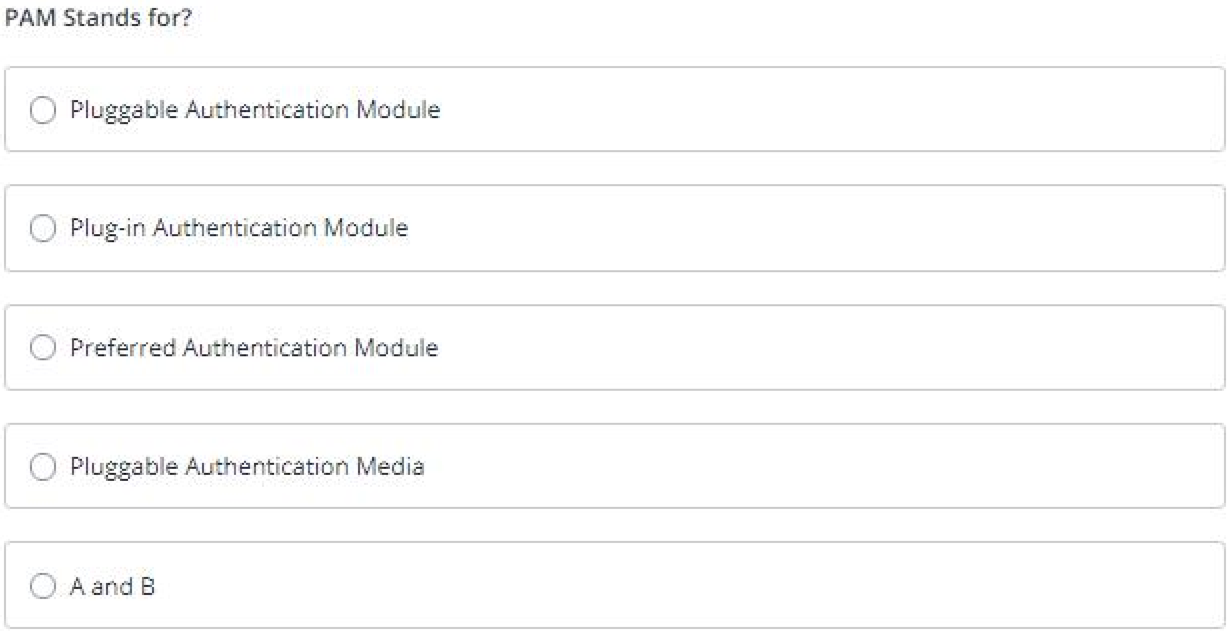
○ setfacl -b path/to/file

○ setfacl -x path/to/file

○ setfacl -x ALL /path/to/file

○ getfacl -b path/to/file

50



PAM Stands for?

○ Pluggable Authentication Module

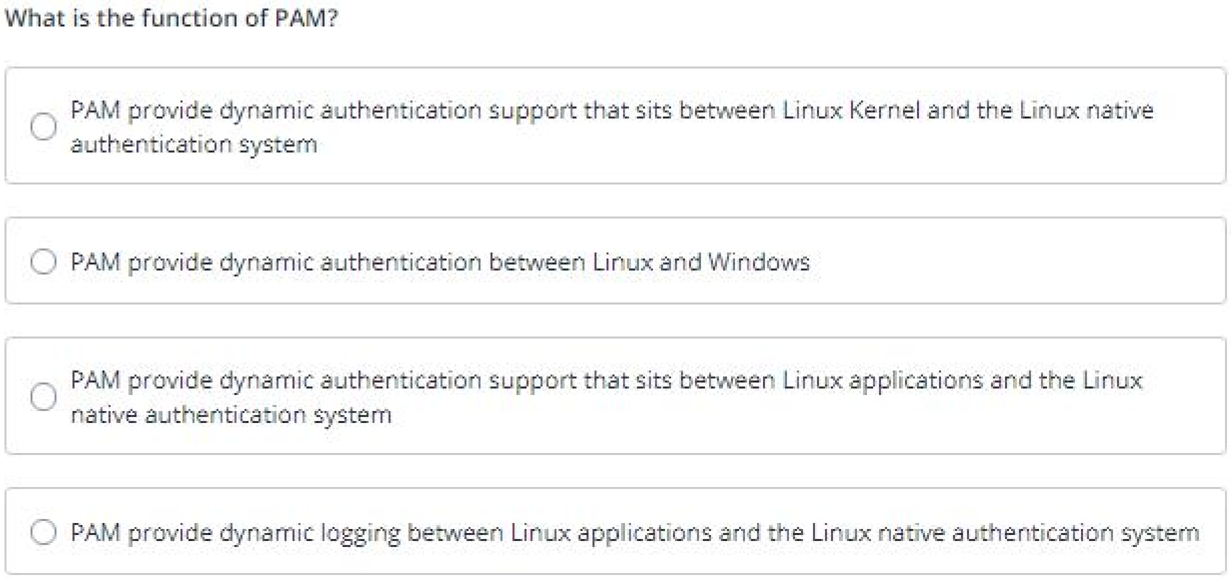
○ Plug-in Authentication Module

○ Preferred Authentication Module

○ Pluggable Authentication Media

○ A and B

51



What is the function of PAM?

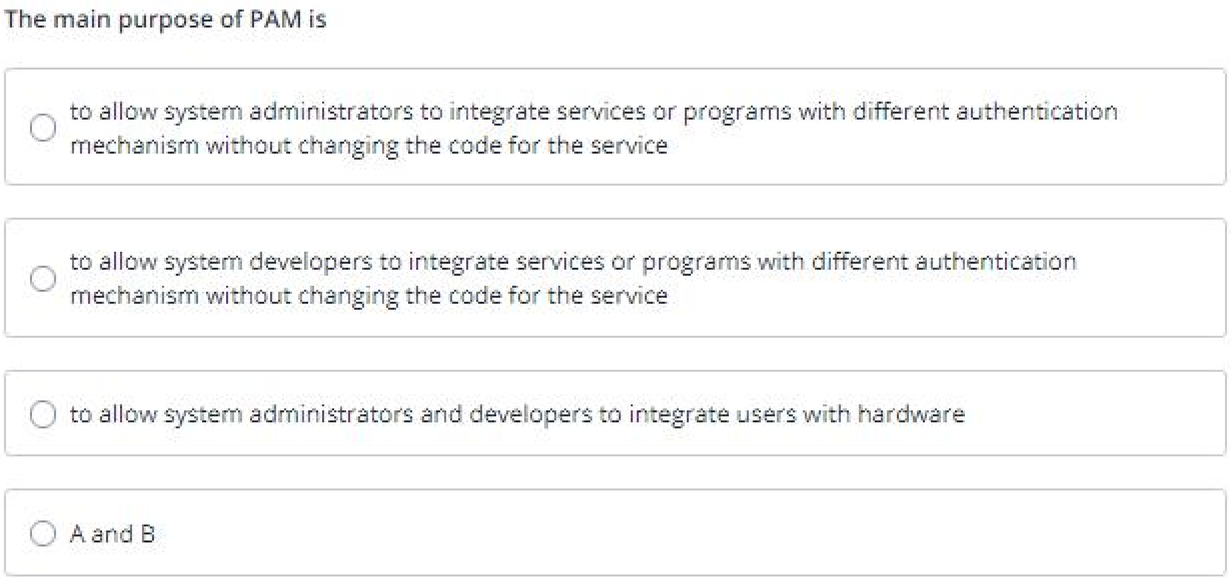
○ PAM provide dynamic authentication support that sits between Linux Kernel and the Linux native authentication system

○ PAM provide dynamic authentication between Linux and Windows

○ PAM provide dynamic authentication support that sits between Linux applications and the Linux native authentication system

○ PAM provide dynamic logging between Linux applications and the Linux native authentication system

52



The main purpose of PAM is

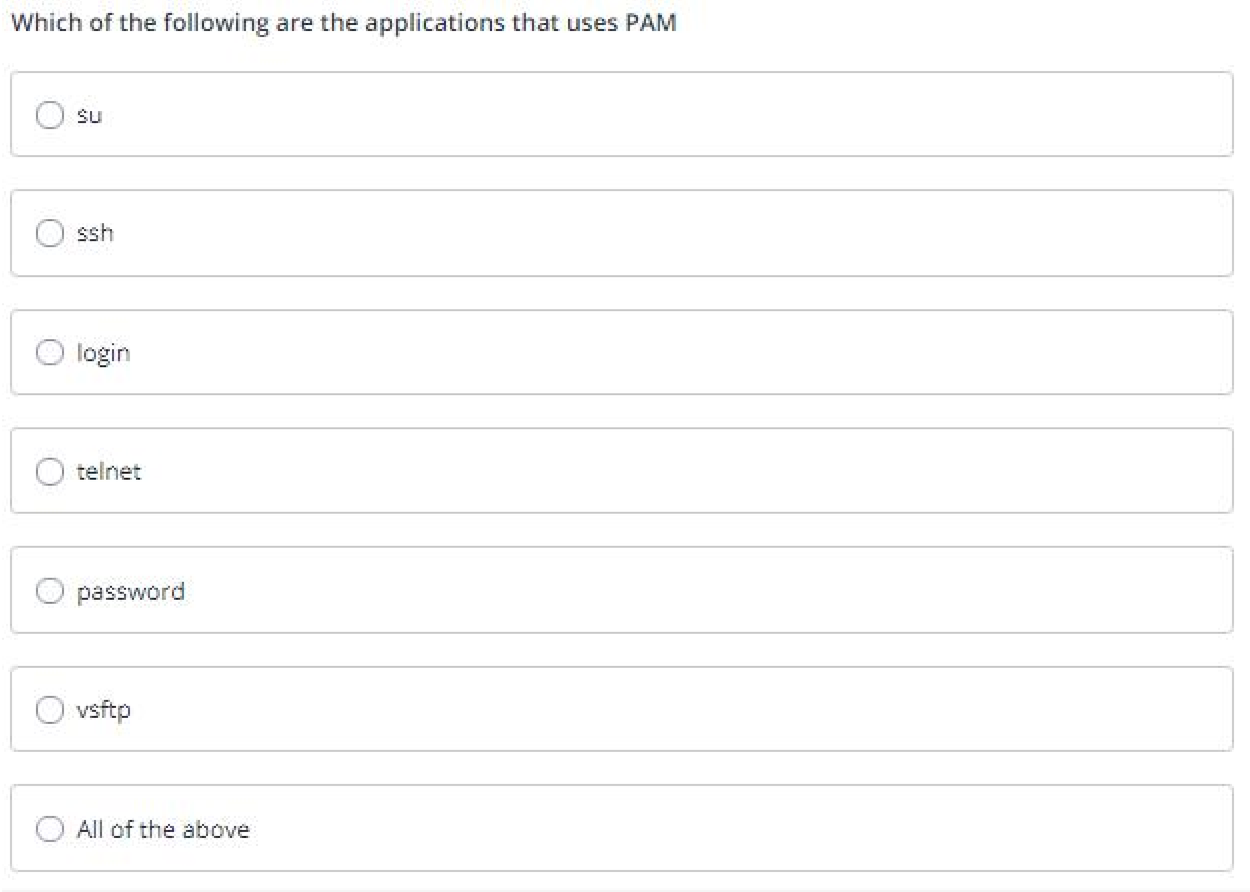
○ to allow system administrators to integrate services or programs with different authentication mechanism without changing the code for the service

○ to allow system developers to integrate services or programs with different authentication mechanism without changing the code for the service

○ to allow system administrators and developers to integrate users with hardware

○ A and B

53



Which of the following are the applications that uses PAM

○ su

○ ssh

○ login

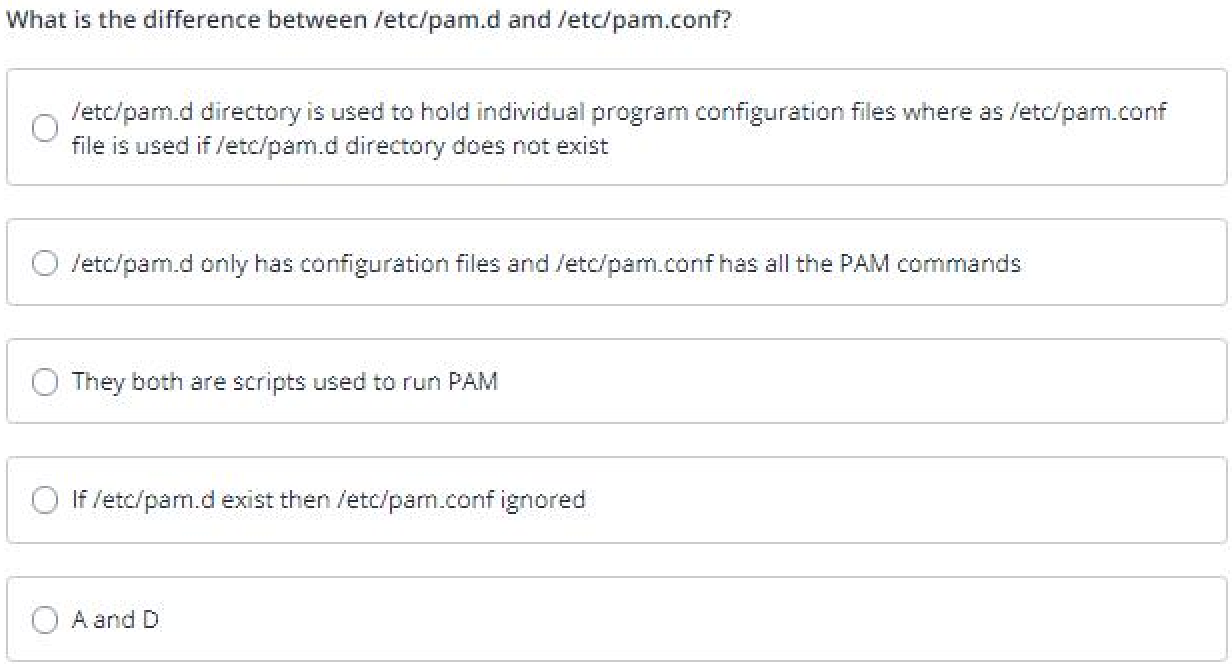
○ telnet

○ password

○ vsftp

○ All of the above

54



What is the difference between /etc/pam.d and /etc/pam.conf?

○ /etc/pam.d directory is used to hold individual program configuration files where as /etc/pam.conf file is used if /etc/pam.d directory does not exist

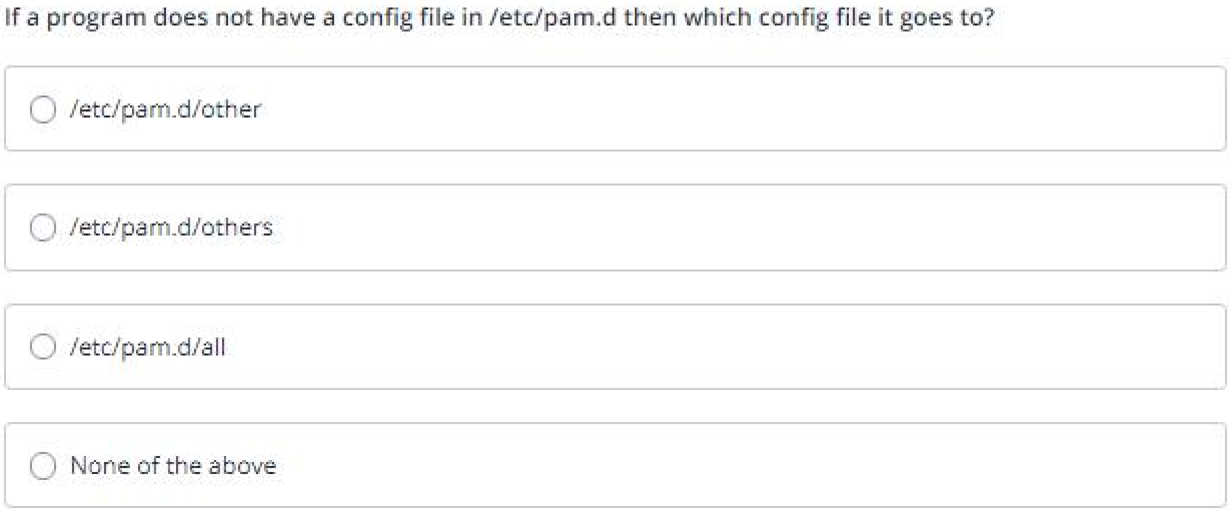
○ /etc/pam.d only has configuration files and /etc/pam.conf has all the PAM commands

○ They both are scripts used to run PAM

○ If /etc/pam.d exist then /etc/pam.conf ignored

○ A and D

55



If a program does not have a config file in /etc/pam.d then which config file it goes to?

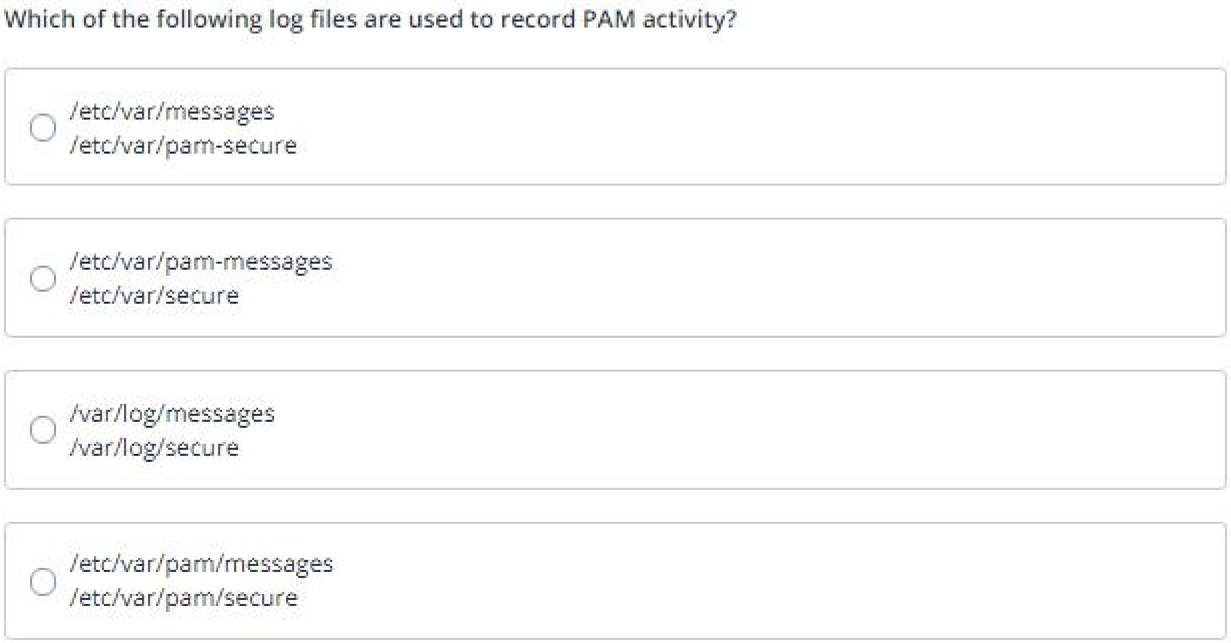
○ /etc/pam.d/other

○ /etc/pam.d/others

○ /etc/pam.d/all

○ None of the above

56



Which of the following log files are used to record PAM activity?

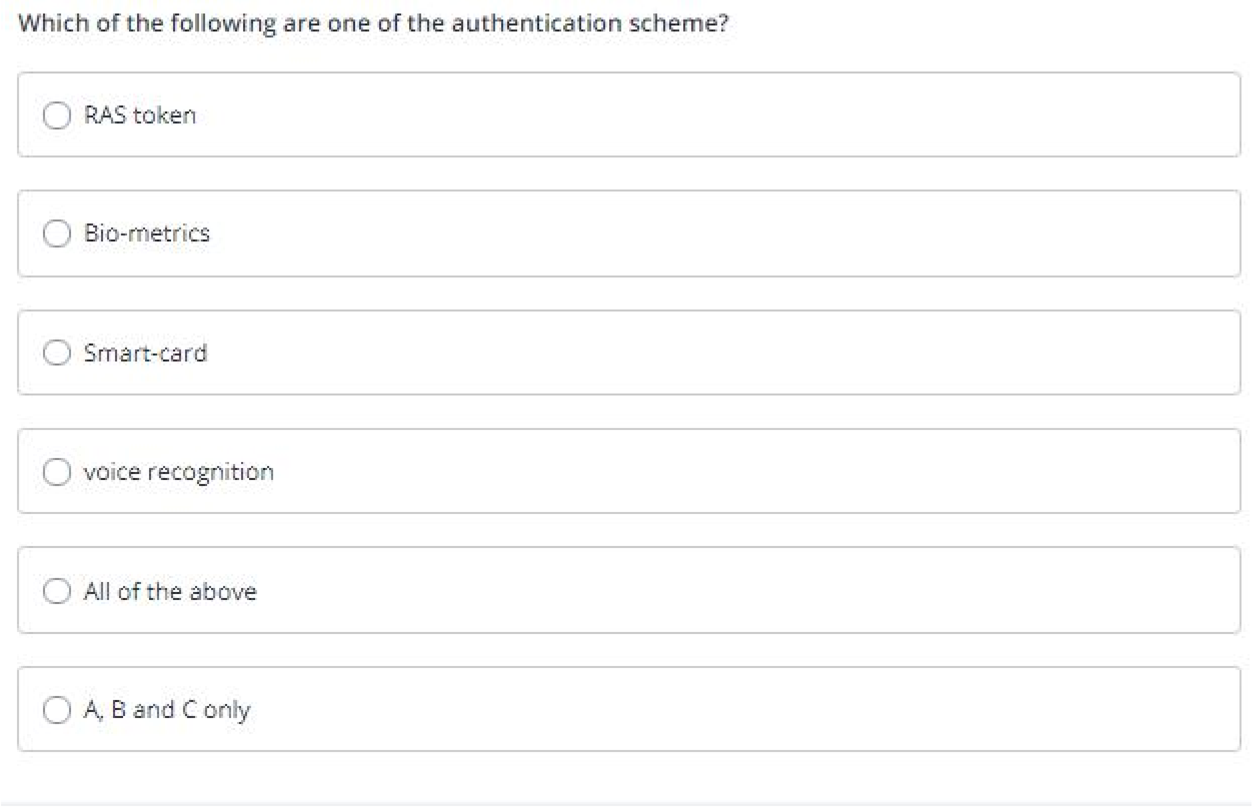
○ /etc/var/messages
/etc/var/pam-secure

○ /etc/var/pam-messages
/etc/var/secure

○ /var/log/messages
/var/log/secure

○ /etc/var/pam/messages
/etc/var/pam/secure

57



Which of the following are one of the authentication scheme?

○ RAS token

○ Bio-metrics

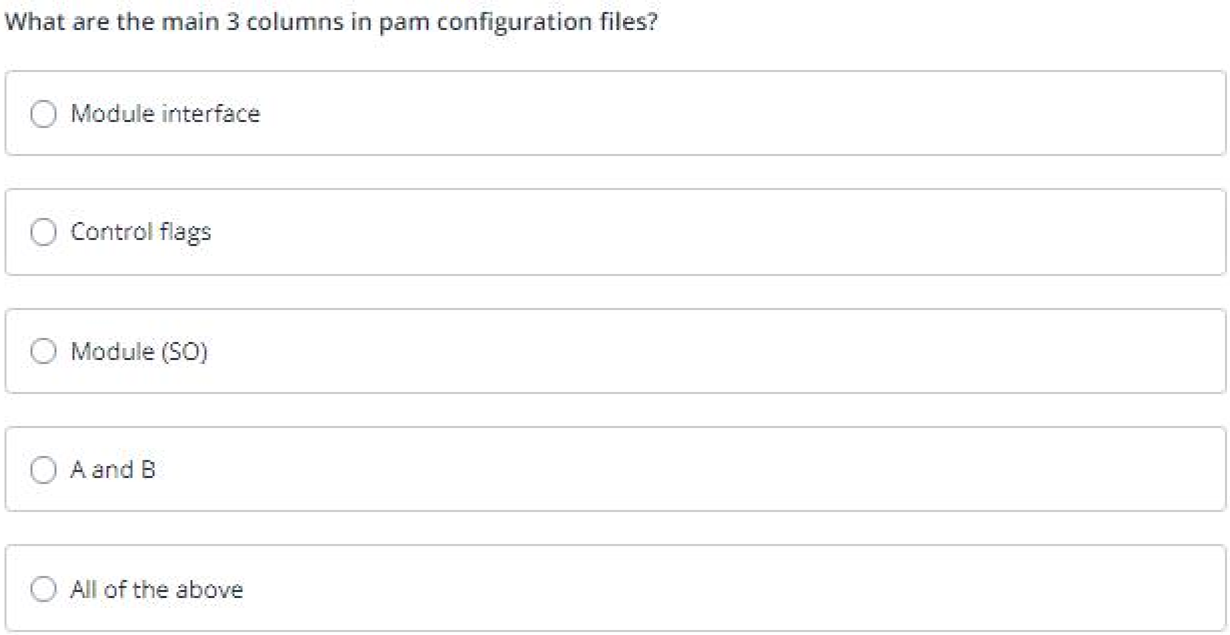
○ Smart-card

○ voice recognition

○ All of the above

○ A, B and C only

58



What are the main 3 columns in pam configuration files?

○ Module interface

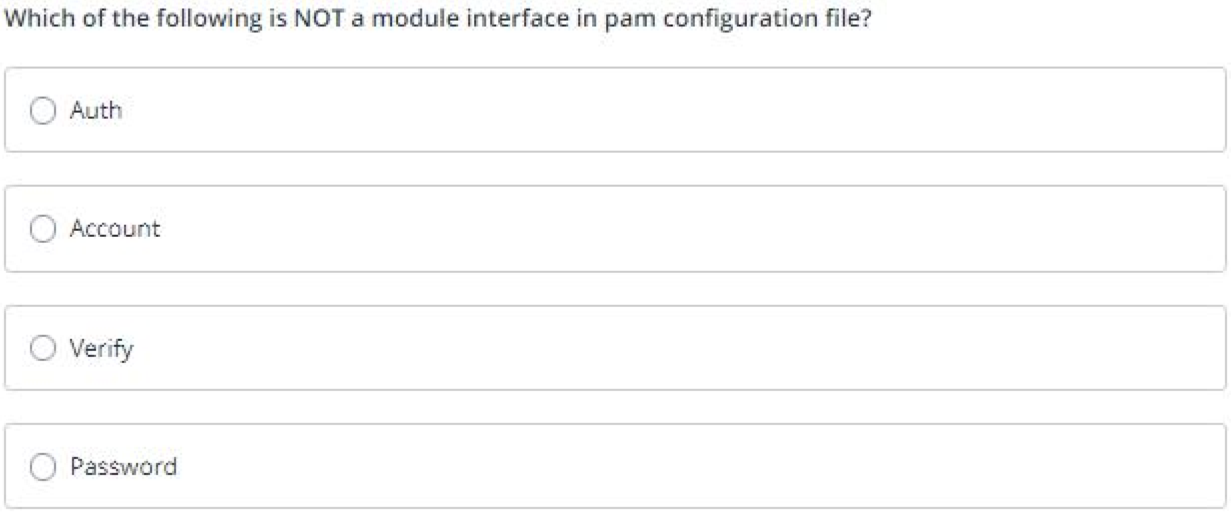
○ Control flags

○ Module (SO)

○ A and B

○ All of the above

59



Which of the following is NOT a module interface in pam configuration file?

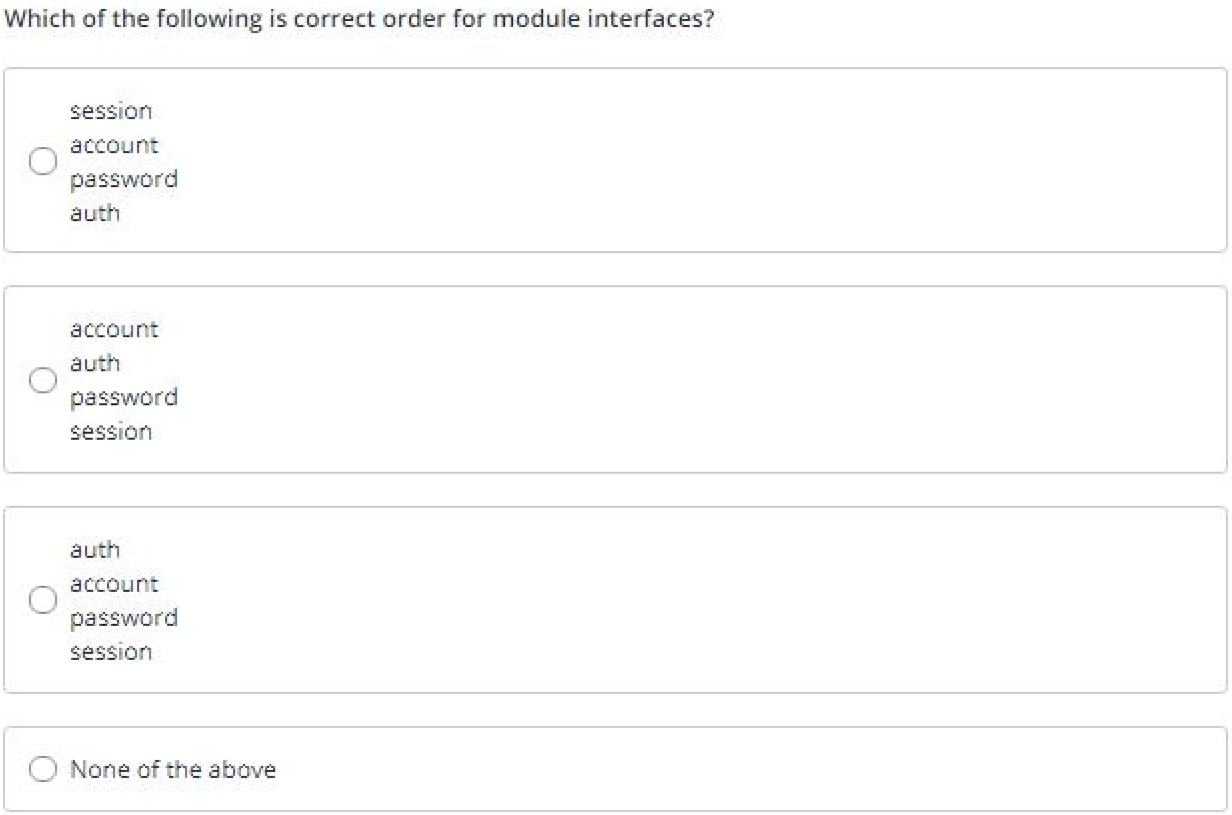
○ Auth

○ Account

○ Verify

○ Password

60



Which of the following is correct order for module interfaces?

○ session
account
password
auth

○ account
auth
password
session

○ auth
account
password
session

○ None of the above