

DUMPS ARENA

Linux Security

ECCouncil 212-77

Version Demo

Total Demo Questions: 8

Total Premium Questions: 51

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following practices is the most useful physical security requirement for a Linux server?

- A. Keep the Linux server in a locked room.
- B. Never leave the Linux computer unattended while it is running.
- C. Maintain a password-protected screensaver on the Linux server.
- D. Keep passwords stored in a locked file cabinet.

ANSWER: D

QUESTION NO: 2

Which statement describes the cron daemon?

- A. Manages scheduling of routine system tasks
- B. Manages all incoming connections and spawns off child processes
- C. Is responsible for file sharing across a network
- D. Keeps track of system messages and errors
- E. Manages the printing subsystem

ANSWER: B

QUESTION NO: 3

Which of the following statements applies to the IP address 192.168.0.1?

- A. It is reserved.
- B. It cannot be assigned to a host that accesses the Internet.
- C. It is designated for multicast transmission.

D. It can be freely assigned to a host on a private network

ANSWER: A

QUESTION NO: 4

Which of the following is not a Linux DHCP client?

- A. dhcpcd
- B. pump
- C. dhcpd
- D. dhclient

ANSWER: A

QUESTION NO: 5

Which of the following types of information is returned by typing `ifconfig eth0`?

(Choose two)

- A. The names of programs that are using `eth0`
- B. The IP address assigned to `eth0`
- C. The hardware address of `eth0`
- D. The hostname associated with `eth0`

ANSWER: B D

QUESTION NO: 6

Which of the following configuration options for kernel enable you to effectively make your computer a router?

- A. `CONFIG_FIREWALL`
- B. `CONFIG_IP_FIREWALL`
- C. `CONFIG_SYN_COOKIES`

D. CONFIG_IP_FORWARD

ANSWER: A

QUESTION NO: 7

A computer is chained firmly to the wall, all of its accounts are secured with good shadowed passwords, and it's configured to boot only from its hard disk, but the system has no BIOS or boot loader password. No users are currently logged into this system. How might a malicious individual without an account on this system corrupt it if given a few minutes alone with it? (Choose two)

- A.** The intruder could reboot it, reconfigure it to boot from floppy, boot a DOS floppy, and use DOS's disk utilities to delete the Linux partitions and erase the hard disk.
- B.** The intruder could open the case, remove the hard disk and insert it in another computer, then modify the configuration files and return the hard disk to the original machine.
- C.** The intruder could run a password-cracking program on the system's `/etc/passwd` file, thus obtaining all the user's passwords for use in further compromising the system at a later date.
- D.** The intruder could utilize a bug in `su`, `passwd`, or some other SUID root program to acquire root privileges and then alter the system's configuration files.

ANSWER: A B

QUESTION NO: 8

Which of the following are risks of SUID and SGID programs? (Choose two)

- A.** Bugs in the programs may cause more damage than they would in ordinary programs.
- B.** The program files are large and thus may cause a disk to run out of space.
- C.** Because the programs require password entry, running them over an insecure network link runs the risk of password interception.
- D.** Users may be able to abuse a program's features, thus doing more damage than would otherwise be possible.

ANSWER: B D