DUMPSQUEEN

Linux Security

ECCouncil 212-77

Version Demo

Total Demo Questions: 8

Total Premium Questions: 51

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

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: 2

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: 3

What would the following command do?

cat MyFile | sort | tee | lpr

A. Print the contents of MyFile in alphabetical order and display the contents of MyFile in sorted order.

B. Print the contents of MyFile in alphabetical order and display the contents of MyFile.

C. It would not work because it contains too many pipes.

D. Print the contents of MyFile in alphabetical order.

ANSWER: A

QUESTION NO: 4

How should you engage users in helping to secure your computer's passwords?

A. Educate them about the importance of security, the means of choosing good passwords, and the ways crackers can obtain passwords.

B. Instruct your users to e-mail copies of their passwords to themselves on other systems so that they're readily available in case of an emergency

C. Enforce password change rules but don't tell users how crackers obtain passwords since you could be educating a future cracker.

D. Give some of your users copies of the encrypted database file as backup in case a cracker breaks in and corrupts the original.

ANSWER: A

QUESTION NO: 5

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

QUESTION NO: 6

You're using a communications protocol that cannot handle encrypted passwords.

You need to disable the Shadow Password Suite. Which of the following pairs of commands restores the original clear-text passwords that you had encrypted into the

/etc/shadow and /etc/gshadow files?

A. grpunconv; passunconv

B. grpunconv; pwunconv

C. gconv; passunconv

D. gconv; pwunconv

ANSWER: B

QUESTION NO: 7

You add the following line to the /etc/passwd file mary12250Mary

Jones/home/mary/bin/bash a

and use the passwd command to change her password. You also create her home directory. However, when Mary tries to log in, the login fails. What is the problem?

A. You did not assign a valid password to Mary's account.

B. You did not set the appropriate permissions to her home directory.

C. You did not create her home directory.

D. You cannot create a new user account by manually editing the /etc/passwd file.

ANSWER: C

QUESTION NO: 8

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