Name: _____ **Class:** _____ **Date:** _____ **ID: A**

POP Quiz #5, Pt. 2

Multiple Choice
Identify the choice that best completes the statement or answers the question.

1. A file has a -rwxrwxrwx permission string. A system administrator issues the chmod u=rw filename command. What will be the new permission string of the file after the given command is issued?

   a. -rw-rwxrwx
   b. -rwxrwxrw-
   c. -rwxrw-rwx
   d. -rw-rw-rw-

2. You discover that an old version of a Debian application is being installed by users. You need to remove the package and its configuration files using the dpkg command. Which parameter should you use?

   a. -p
   b. -r
   c. -P
   d. -R

3. A Linux user issues the ls -l command and obtains the following output on the screen:
   -rw-rw---- 34 salary finance 42 Jun 18 18:01 sal
   Which explanation is most accurate?

   a. The user finance is the owner of the file named salary, which belongs to a group named sal. The file size is 34 bytes, and 42 hard links exist for this file.
   b. The user salary is the owner of the file named sal, which belongs to a group named finance; the file size is 42 bytes, and 34 hard links exist for this file.
   c. The user finance is the owner of the file named sal, which belongs to a group named salary. The file size is 42 bytes, and 34 hard links exist for this file.
   d. The user sal is the owner of the file named salary, which belongs to a group named finance. The file size is 34 bytes long, and 42 hard links exist for this file.

4. Which of the following is it wise to do when deleting an account with userdel?

   a. Ensure that the user's password isn't duplicated in /etc/passwd or /etc/shadow.
   b. Search the computer for stray files owned by the former user.
   c. Change permissions on system files to prevent the user from accessing them remotely.
   d. Delete the user's files with a utility that overwrites former file contents with random data.

5. An ls -l command reveals that the loud file has a permission string of crw-rw---- and ownership by the user root and group audio. Which of the following is a true statement about this file?

   a. Only root and the account that created it may read or write the file.
   b. The file is a directory, as indicated by the leading c.
   c. Anybody in the audio group may read from and write to the file.
   d. The command chmod 660 loud will make it accessible to more users.

6. Under which of the following circumstances will a chmod command not work?

   a. The user issuing the command doesn't own the file but does own and have write permission to the directory in which the file resides.
   b. The root user issues the command on a file that resides in a read/write filesystem, although the file itself has no write permissions active.
   c. The owner of the file issues the command, but the file's permissions don't grant the owner write access to the file.
   d. The owner of the file issues the command, but the file resides in a directory to which the owner has read but not write access.

7. What is the function of the su command?

   a. It gives the named user superuser privileges.
   b. It acquires the named user's privileges, or the superuser's if no username is specified.
   c. It acquires superuser privileges for the user who runs the command.
   d. It gives everybody currently logged in superuser privileges.

8. Which category of attack denies you the use of your equipment?

   a. DoS
   b. Core
   c. Rooted
   d. Phish

9. Which of the following commands displays the contents of a tarball, including file sizes and time stamps?

   a. tar xzf theprogram-1.2.3.tgz
   b. tar tzf theprogram-1.2.3.tgz
   c. tar tvzf theprogram-1.2.3.tgz
   d. tar x theprogram-1.2.3.tgz

10. Which of the following commands replaces jpertwee's current cron job with my-cron?

    a. crontab -r my-cron
    b. crontab -e my-cron
    c. crontab jpertwee my-cron
    d. crontab -u jpertwee my-cron

11. Which of the following lines, if used in a user cron job, will run /usr/local/bin/cleanup twice a day?

    a. 15 7,19 * * * tbaker /usr/local/bin/cleanup
    b. 15 7,19 * * * /usr/local/bin/cleanup
    c. 15 */2 * * * tbaker /usr/local/bin/cleanup
    d. 15 */2 * * * /usr/local/bin/cleanup

12. What is wrong with the following system cron job entry (in /etc/crontab)?
    17 * * * * run-parts /etc/cron.hourly

    a. This command should run hourly but will run only at 5:00 p.m
    b. There is no run-parts command in Linux.
    c. The time specification is incomplete.
    d. It's missing a user specification.

13. A user creates a cron job to retrieve e-mail from a remote server using the fetchmail program. What is true of this cron job, if it's properly configured?

    a. The fetchmail process runs with the UID of the user who created the cron job.
    b. The fetchmail process runs with the root UID.
    c. The fetchmail process runs with the crontab UID.
    d. The fetchmail process runs with the nobody UID.

14. What is the purpose of the /etc/sysctl.conf file?

    a. It holds miscellaneous system configuration options that are set via the sysctl utilitywhen the system boots.
    b. It specifies the order in which system services are started when the computer boots.
    c. It specifies the filesystems that are mounted at boot time or that may be mounted man- ually by ordinary users.
    d. It identifies system services that are started directly by the init process when the com- puter boots.

15. Which of the following configuration files does the logrotate program consult for its settings?

    a. /etc/logrotate.conf
    b. /usr/sbin/logrotate/logrotate.conf
    c. /usr/src/logrotate/logrotate.conf
    d. /etc/logrotate/.conf

16. Which of the following commands will change all occurrences of dog in the file animals.txt to mutt in the screen display?

    a. sed –s “dog” “mutt” animals.txt
    b. grep –s “dog||mutt” animals.txt
    c. sed ‘s/dog/mutt/‘ animals.txt
    d. cat animals.txt | grep –c “dog” “mutt”

17. Which of the following umask values will result in files with rw-r----- permissions?

    a. 640
    b. 210
    c. 022
    d. 027

18. In performing your administrative duties, you’ve made heavy use of the su command to temporarily acquire various users’ identities, and you’ve forgotten with which account a shell is currently associated. How might you resolve this question?

    a. Type whoami.
    b. Type cat /etc/passwd.
    c. Select File User from the desktop environment’s menu.
    d. Type bash to start a new shell.

Multiple Response
Identify one or more choices that best complete the statement or answer the question.

19. Which of the following types of information are you likely to see in log files?

    a. Information about a user launching a text editor to edit a file in the user’s directory.
    b. Successful uses of the su command to acquire root privileges
    c. Failed attempts to log in to a server controlled through xinetd
    d. Failed attempts by a user to read another user’s files via the cat command

20. You discover that a process with PID 27319 is running out of control, consuming most of the system’s CPU time when it shouldn’t be. As root, you type kill -15 27319, but the process continues to run. What might you try next?

    a. Type **kill -9 27319**
    b. Type **kill -TERM 27319**
    c. Type **kill -KILL 27319**
    d. Type **killall 27319**

21. Which of the following tasks is likely to be handled by a cron job?

    a. Starting an important server when the computer boots
    b. Finding and deleting old temporary files
    c. Scripting supervised account creation
    d. Monitoring the status of servers and e-mailing a report to the superuser

POP Quiz #5, Pt. 2
Answer Section

MULTIPLE CHOICE

1. ANS: A PTS: 1
2. ANS: C PTS: 1
3. ANS: B PTS: 1
4. ANS: B
   Tracking down and removing or changing the permissions of a former user's files can prevent confusion or possibly even spurious accusations of wrongdoing in the future. Unless the user was involved in system cracking, there's no reason to think that the user's password would be duplicated in the password database. No system file's ownership or permissions should need changing when deleting a user. Although overwriting deleted files with random data may be useful in some high-security environments or with unusually sensitive data, it's not a necessary practice on most systems. See Chapter 5 for more information.

   PTS: 1
5. ANS: C
   The second set of permission bits (rw-) indicates that the file's group (audio) may read from and write to the file. This permission string ensures that, if audio has more than one member, multiple users may access the file. The leading c indicates that the file is a char- acter device file, not a directory. The command chmod 660 loud will not change the file's permissions; 660 is equivalent to rw-rw----.

   PTS: 1
6. ANS: A
   Only the file's owner and root may change permissions on a file via chmod. Whether the file is writeable by the owner is irrelevant, as is whether the directory in which the file resides is writeable.

   PTS: 1
7. ANS: B
   Typing su username gives the person who runs the command the privileges associated with that username, assuming that the person who runs the command successfully enters the user's password. When the username isn't specified, root is assumed. The su command also runs a program as the specified user. Normally, this is a shell, but you can specify another program using a command-line argument. Although option C describes part of what su can do, option C is incomplete; option B is a more complete answer. The su com- mand does not give superuser privileges to the named user, nor does it give everybody who's logged in superuser privileges.

   PTS: 1
8. ANS: A
   A denial of service (DoS) attack is any type of attack that denies you the use of your equipment. Core is not a type of attack. Rooted is a term used to describe root access being obtained by a hacker, while phishing involves sending bogus e-mails or setting up fake Web sites that lure unsuspecting individuals into divulging sensitive financial or other informa- tion.

   PTS: 1

9. ANS: C
Option A extracts files from the archive without displaying their names. Option B lists the files in the archive, but without the --verbose (v) option, it doesn't list file sizes or time stamps. Option D will cause tar to attempt to extract the named file from its standard tape device. See Chapter 7 for more information.

PTS: 1

10. ANS: D
The -r option removes a user's cron job, and the -e option edits the user's cron job.Any parameter following either of these is interpreted as a username, so both options A and B interpret my-cron as the username. Option C is malformed, but it will have the effect of installing the file jpertwee as the cron job for the user who types the command. The-u jpertwee parameter in option D correctly specifies the user as jpertwee, and the last parameter (my-cron) is the file holding the cron job specification.

PTS: 1

11. ANS: B
User cron jobs don't include a username specification (tbaker in options A and C). The */2 specification for the hour in options C and D causes the job to execute every other hour; the 7,19 specification in options A and B causes it to execute twice a day, on the 7th and 19th hours (in conjunction with the 15 minute specification, that means at 7:15 a.m. and 7:15 p.m.).

PTS: 1

12. ANS: D
System cron jobs require a user specification after the time specification and before the command to be executed, and this entry is missing in this specification. (This entry would be legal for a user cron job, though, assuming the user could run the command.) Option A is incorrect because the time specification runs the job at 17 minutes past the hour, every hour; and even if it did run at 5:00 p.m., the entry would be legal, if confusingly named. Option B is incorrect because run-parts, although not present on all Linux distributions, is used on several distributions. Cron is also capable of running user-written scripts and programs, so even if run-parts weren't a standard Linux utility, the entry would still work if you'd written your own run-parts script. Option C is incorrect because the time specifi- cation is complete; it includes a minute value (17) and asterisks (*) denoting a run at every hour, day of the month, month, and day of the week.

PTS: 1

13. ANS: A
User cron jobs run as the user who created them, so option A is correct.

PTS: 1

14. ANS: A
Option A correctly describes the purpose of /etc/sysctl.conf. Option B is a partial description of the purpose of SysV init scripts. Option C describes the function of the /etc/ fstab file. Option D describes the purpose of the /etc/inittab file.

PTS: 1

15. ANS: A
The logrotate program consults a configuration file called /etc/logrotate.conf, which includes several default settings and typically refers to files in /etc/logrotate.d to handle specific log files.

PTS: 1

16. ANS: B
The sed utility can be used to “stream” text and change one value to another. In this case, the s option is used to replace dog with mutt. The syntax in option A is incorrect, while options B and D are incorrect since grep does not include the functionality needed to make the changes.

PTS: 1

17. ANS: D
Option D, 027, removes write permissions for the group and all world permissions. (Files normally don’t have execute permissions set, but explicitly removing write permissions when removing read permissions ensures reasonable behavior for directories.) Option A, 640, is the octal equivalent of the desired rw-r----- permissions, but the umask sets the bits that areto be removed from permissions, not those that are to be set. Option B, 210, would remove write permission for the owner, but it would not remove write permission for the group, which is incorrect. This would also leave all world permissions open. Finally, option C, 022, would not remove world read permission.

PTS: 1

18. ANS: A
The whoami command displays the effective user ID—the username associated with the command, which will in turn be the username associated with the current shell. Option B will display the current account database file, but this information won’t help answer the question of what account you’re using. Even if a desktop environment has a File User menu item, that item won’t reliably tell you whose account you’re using at a command shell. Any shell you launch from the current one will run with the current shell’s privileges, so option D won’t be effective.

PTS: 1

MULTIPLE RESPONSE

19. ANS: B, C
Log files record messages generated by the kernel, servers, and certain security- related system utilities. The su command typically records a summary of its actions in log files, and xinetd typically records login failures, although these defaults can be changed. Text editors seldom log information, nor do simple file-viewing utilities, even if they’re asked to violate file security measures.

PTS: 1

20. ANS: A, C
A, C. Signal 15, passed to process 27319 by typing kill -15 27319, terminates well- behaved processes but sometimes fails when processes are out of control. Options A andC both pass signal 9 (aka SIGKILL) to the process, which is more likely to work with an out-of-control process but gives the process no chance to shut down cleanly. Another name for signal 15 is SIGTERM, so option B is exactly equivalent to the original commandthat failed to work. The killall command of option D terminates processes by name, so option D will attempt to terminate any process with a name (but not a PID) of 27319. Fur- thermore, killall (like kill) sends a signal 15 by default, so even if PID 27319 happens to be named 27319, option D won’t have any more effect than the original command or option B.

PTS: 1

21. ANS: B, D
Cron is a good tool for performing tasks that can be done in an unsupervised man- ner, like deleting old temporary files or checking to see that servers are running correctly. Tasks that require interaction, such as creating accounts, are not good candidates for cron jobs, which must execute unsupervised. Although a cron job could restart a crashed server, it's not normally used to start a server when the system boots; that's done through SysV startup scripts or a super server.

PTS: 1