

Name _____

Exam #1

CIS 68C1-01

Fall 2001

Instructions

- Write your name at the top of every sheet.
- For **True/False** and **Multiple Choice** questions, *circle* the single correct answer (true or false, or one of the appropriate letters a – e).
- For **Short Answer** questions, write your answer in the space provided. I will not work very hard to figure out what you *mean* to say, so be as specific as you possible. Otherwise you run the risk of receiving no credit or only partial credit.
- There is no penalty for incorrect answers

Name _____

True / False

1. A system administrator is responsible for the following duties: system security, backups, adding new users, adding new hardware, installing and configuring software, maintaining local documentation, troubleshooting, and monitoring the system. (True / False)
2. If you increase the **nice** value of a process by 10, the UNIX kernel will give more time to the process. (True / False)
3. A user's EUID determines a user's identify. (True / False)
4. The `/etc/shadow` file is used on all UNIX systems. (True / False)
5. IDE supports 8 devices. (True / False)
6. You change a user's UID with the **setuid** command. (True / False)
7. The **insmod** command will resolve and load all module dependencies. (True / False)
8. To make a file readable by another user, user *sally* could use the **chown** command. (True / False)
9. After making changes to the file `/etc/lilo.conf`, you must reboot. (True / False)
10. The partition boot record uses the master boot record to boot a system. (True / False)
11. System administrators should generally keep a root terminal session (eg. xterm) open and available for emergency needs. (True / False)
12. You can resolve the problem of a filesystem running out of inodes using the **fsck** command. (True / False)
13. The command **ps -ef jane** will give a listing of only the process owned by user *jane*. (True / False)
14. The file `/etc/modules.conf` is used to list all the LKMs in the system. (True / False)
15. The Linux installer runs under DOS from the installer boot floppy. (True / False)
16. The predominant disk format in the PC world is SCSI. (True / False)
17. For a single-boot system, it is acceptable to install LILO into the alternate boot record. (True / False)
18. A **setuid** process runs with the users EUID and the program owner's UID. (True / False)
19. The command **fsck /dev/swap** will usually resolve any corruption found in the filesystem. (True / False)
20. In Linux, networking devices have device entries in `/dev`. (True / False)

Multiple Choice

21. The maximum number of primary partitions for IDE hard disks?
 - a. 3
 - b. 4
 - c. 7
 - d. 8

Name _____

22. The **mknod** utility is used to create which of the following?
- a. mount points
 - b. symbolic links
 - c. **device files**
 - d. networking connections
23. Which of the following commands would create a new Linux file system?
- a. `mkfs -t ext2 /mnt/hda0`
 - b. `fsck -t ext2 /mnt/fd`
 - c. **`mkfs -t ext2 /dev/hda3`**
 - d. both (a) and (c)
24. What would be an appropriate **netmask** given the IP address 140.123.0.10 and broadcast address 140.123.255.255?
- a. 255.255.255.0
 - b. **255.255.0.0**
 - c. 0.0.255.255
 - d. 255.255.255.255
25. The IP address 127.0.0.1 is: _____
- a. localhost
 - b. **the loopback network pseudo-device**
 - c. a DHCP assigned network number
 - d. a netmask

26. The output below is from an `ls -l` command. What type of file is the file below?

```
brw-rw---- 1 root disk      3, 66 Aug 24 2000 hdb2
```

- a. **block**
 - b. binary
 - c. ASCII or text
 - d. character device
 - e. raw
27. What file does the following line belong to:
- ```
root:1CSOuObD5$GUFtSp.Ma9kU2RclbqDDG.:7305:0:99999:7:::
```
- a. `/etc/passwd`
  - b. **`/etc/shadow`**
  - c. `/etc/inittab`
  - d. none of the above
28. Which of the following statements is *not* correct?
- a. the KILL signal cannot be caught or blocked
  - b. the ABORT signal will terminate a process, unless the process has blocked the signal
  - c. the TERM and QUIT signals can be caught and blocked
  - d. the STOP signal cannot be caught or blocked
  - e. **all are correct**
29. Which of the following `rc.d` startup directories are used when booting to multi-user mode?
- a. `/etc/rc.d/rc1.d`
  - b. `/etc/rc.d/rc2.d`
  - c. **`/etc/rc.d/rc3.d`**
  - d. all of the above

Name \_\_\_\_\_

30. The partial output below is from a **ps -ef** command. What command would you give to terminate the process *runaway*?

```
UID PID PPID C STIME TTY TIME CMD
sam 532 530 0 11:56 tty1 00:01:23 /home/smith/runaway -9
```

- a. kill -9 530
- b. kill -TERM 532
- c. kill -9 runaway
- d. kill -15 -1
- e. kill -9 532

### Short Answer

31. With **umask** set to *022*, what would the permissions be on newly created files and directories? \_\_\_\_\_

New files: 644

New directories: 755

32. List two primary causes of installation failure during the mini-Linux boot stage? \_\_\_\_\_

Device incompatibility. Device conflict. Unsupported devices. IRQ conflicts. Device I/O conflicts.

33. The **tty** device has major number 4. Give the full path of the device with major number 4, minor number 4? \_\_\_\_\_

/dev/tty4

34. Is it safe to shut down UNIX by just turning off the power to the system? Explain your answer. \_\_\_\_\_

No, it is not safe. The UNIX filesystem is a cached filesystem. Changes to the filesystem are not written to disk immediately, and are periodically flushed. Turning of the power is likely to cause filesystem corruption as any changes still in RAM will not have been flushed to the disk.

35. You are logged into your normal, non-root account. You want to check that the new user account you added to the system is in the */etc/shadow* file. You briefly **su** to root and you change the file's permissions to *666* using the **chmod** command so that you can look at the file without having to **su**. Is this acceptable? Explain your answer. \_\_\_\_\_

It is unacceptable. Never grant read or write (or execute if meaningful) permissions of restricted files such as */etc/shadow* to non-root users. This is a gaping security hole, allowing non-root users to compromise system security.

36. Jane, a junior system administrator just added a new user to the system. You want to check her work. Below is the listing (from **ls -la**) of the home directory for *joe1234*, the new user. How well did Jane do? Explain your answer.

```
total 20
drwxr-xr-x 2 joe1234 cis68 4096 May 12 12:50 .
drwxr-xr-x 5 joe1234 cis68 4096 May 12 12:48 ..
-rw-r--r-- 1 joe1234 cis68 24 May 12 12:48 .bash_logout
-rw-r--r-- 1 joe1234 cis68 230 May 12 12:48 .bash_profile
-rw-r--r-- 1 joe1234 cis68 124 May 12 12:48 .bashrc
-rw-r--r-- 1 root root 0 May 12 12:50 test
```

Jane made two mistakes, one minor and one major. The major mistake is that she changed the parent directory of *joe1234*'s home directory to be owned by *joe1234*. If *joe1234*'s home directory is */home/joe1234*, then *joe1234*

Name \_\_\_\_\_

would now be the owner of **/home**. Jane also set the group ID of the parent directory to that of joe's primary group **cis68**.

The other problem, which is minor, is that Jane left a file **test** owned by group in joe1234's home directory.

The permissions on joe1234's home directory are fine - it is up to the site administrator how permissive or restrictive permissions should be on a user's home directory. The user can tighten or loosen permissions as desired.

37. You run the command **su root** to become root so that you can shutdown the system. You try to run the **telinit** command, but receive the error:

```
bash: telinit: command not found
```

What does the error mean? Why did you receive this error message? \_\_\_\_\_

The error means that the **bash** shell could not find the command **telinit**. This occurs because the **PATH** does not include the directory where **telinit** resides. It can also mean that the **telinit** command does not exist, but this is unlikely, given that you know it does and there is nothing in the question to indicate that **telinit** suddenly does not exist.

Using the data in the question, you ran **su root**. The **su** command does not create a *login* shell - instead it just creates a new sub-shell which has the effective user id (EUID) of root. Since the shell is not a *login* shell, the shell does not *source* root's **.profile**. Thus, root's **PATH**, which is setup in **/root/.profile**, is not set. The shell created by **su** will inherit *your* **PATH**, since your **PATH** is an environment variable inherited by all sub-processes of your current shell, including the sub-shell created by the **su** command.

To force **su** to create a *login* shell and thus source the **/root/.profile** command file, you must give **su a -** (dash) argument. The command **su - root** or just **su -** are equivalent.

38. What does the command **kill -15 -1** do? \_\_\_\_\_

The command sends the **TERM** signal to all processes except system processes and the current shell. This is used by the shutdown (**kill**) scripts to ask processes to terminate themselves.

39. You send the **TERM** signal to a process using the **kill** command, but it does not terminate. Why? \_\_\_\_\_

The process is blocking, ignoring, or is catching the **TERM** signal, overriding the default action to terminate.

40. Below is one line from the output of an **ls -la** listing of **/home/joeuser**, the home directory for **joeuser**. Does everything look ok to you? Explain your answer.

```
drwxrwxrwx 2 root root 4096 May 12 12:50 /home/joeuser
```

No, there is a problem. A user's home directory should be owned by the user and its group ID should be the user's primary group.

Note that it is perfectly acceptable (but perhaps not advisable) to have a home directory with permissions of **777**; a user can choose to grant or deny access to any or all of his/her files and directories including the home directory.

41. You and co-worker Fred are both UNIX system administrators at a large company, and habitually stayed log in and routinely do work as root. You noticed that the password file was modified at 6:30pm. You did not touch the password file, and Fred is unavailable. Would you be able to determine if Fred changed the file, or if your system had a break in? Explain your answer. \_\_\_\_\_

This question was discarded due to poor wording.

Name \_\_\_\_\_

The gist of this question was to explore your understanding of how there is very little logging occurring on a UNIX system, and that your only means to determine something like a break in is to infer certain events based on what *is* actually logged. The system can log **su**, **telnet**, and **login** (if configured to do so), but does not log changes to files. There is no special logging of root activities. All you may have to work with is the modification time of a file such as `/etc/passwd` and an entry in a log that indicates an **su**, **telnet**, or **login**. If several people are running as root, there will not be any log indicating that an **su**, **telnet**, or **login** had occurred. This would further frustrate your attempts at determining whether a change to a file or some other activity was performed by an authorized user.

42. What specifically does the command **fsck** do? When should you use it? \_\_\_\_\_

The **fsck** command checks a filesystem's integrity and fixes most corruptions. It should be run after a system crash or other event which does not allow for proper un-mounting of the filesystem. It must be run before the filesystem is mounted and used. This generally requires booting into single user mode and forcibly checking the filesystem using **fsck -f**, and it should be run until **fsck** indicates that the filesystem is error-free.

43. You mount a DOS floppy onto the directory `/mnt/floppy`, and copy some files using the **cp** command. Then you remove the floppy, and bring it to a Windows machine to print out the text files you just copied. You come back to the system later, insert the floppy, and are disappointed that UNIX tells you the floppy filesystem is corrupt. What is a likely cause of corruption? \_\_\_\_\_

The most likely cause was removing the mounted DOS filesystem from UNIX without properly un-mounting the filesystem. You must un-mount a filesystem to give the system a chance to flush any cached data. Otherwise, this practice is likely lead to corruption eventually.

44. What is the standard way to temporarily disable a user's account? \_\_\_\_\_

Either place a `*` in the password file in `/etc/passwd` or `/etc/shadow`, or set the user's default login shell in the `/etc/passwd` file to a program (not a shell script) that displays a message indicating the account has been disabled and exits.

45. What is purpose of the `/etc/hosts` file? \_\_\_\_\_

The `/etc/hosts` file is simple text file that local maps hostnames to IP addresses.