Chapter 4 Notes

I. The ps command shows only the processes that belong to the current user and that are running on the current terminal.

A. $ ps

```
PID  TTY          TIME  CMD
3081 pts/0    00:00:00  bash
3209 pts/0    00:00:00  ps
```

B. The GNU ps command that's used in Linux systems supports three different types of command line parameters:

1. Unix-style parameters, which are preceded by a dash
    a) Examples:
        (1) -A/-e: Shows all processes
        (2) -f: Displays a full format listing
            (a) Information columns:
                (i) UID: The user responsible for launching the process
                (ii) PID: The process ID of the process
                (iii) PPID: The PID of the parent process (if a process is started by another process)
                (iv) C: Processor utilization over the lifetime of the process
                (v) STIME: The system time when the process started
                (vi) TTY: The terminal device from which the process was launched
                (vii) TIME: The cumulative CPU time required to run the process
                (viii) CMD: The name of the program that was started
        (3) -l: Displays a long listing
2. BSD-style parameters, which are not preceded by a dash
3. GNU long parameters, which are preceded by a double dash

II. The top command displays process information similarly to the ps command, but it does it in real-time mode

A. Information columns:
    1. PID: The process ID of the process
    2. USER: The user name of the owner of the process
    3. PR: The priority of the process
    4. NI: The nice value of the process
    5. VIRT: The total amount of virtual memory used by the process
    6. RES: The amount of physical memory the process is using
    7. SHR: The amount of memory the process is sharing with other processes
    8. S: The process status (D = interruptible sleep, R = running, S = sleeping, T = traced or stopped, or Z = zombie)
    9. %CPU: The share of CPU time that the process is using
    10. %MEM: The share of available physical memory the process is using
    11. TIME+: The total CPU time the process has used since starting
    12. COMMAND: The command line name of the process (program started)
B. By default, when you start top, it sorts the processes based on the %CPU value
C. Each interactive command is a single character that you can press while top is running and changes the behavior of the program

III. Linux process signals:
A. HUP: Hangs up
B. INT: Interrupts
C. QUIT: Stops running
D. KILL: Unconditionally terminates
E. SEGV: Produces segment violation
F. TERM: Terminates if possible
G. STOP: Stops unconditionally, but doesn't terminate
H. TSTP: Stops or pauses, but continues to run in background
I. CONT: Resumes execution after STOP or TSTP

IV. The kill command allows you to send signals to processes based on their process ID (PID)
A. By default, the kill command sends a TERM signal to all the PIDs listed on the command line
B. To send a process signal, you must either be the owner of the process or be logged in as the root user

C. The -s parameter allows you to specify other signals (either using their name or signal number)
    1. # kill -s HUP 3940

V. The killall command is a powerful way to stop processes by using their names rather than the PID numbers
    A. Allows you to use wildcard characters

VI. Before you can use a new media disk on your system, you must place it in the virtual directory. This task is called mounting
    A. Most Linux distributions have the ability to automatically mount specific types of removable media
        1. A removable media device is a medium that can be easily removed from the PC, such as CD-ROMs and USB memory sticks
    B. The command used to mount media is called mount
        1. mount -t type device directory
        2. By default, the mount command displays a list of media devices currently mounted on the system
        3. The mount command provides four pieces of information:
            a) The device filename of the media
            b) The mount point in the virtual directory where the media is mounted
            c) The filesystem type
            d) The access status of the mounted media
        4. To manually mount a media device in the virtual directory, you must be logged in as the root user or use the sudo command to run the command as the root user.
        5. The -o option allows you to mount the filesystem with a comma-separated list of additional options
            a) ro: Mounts as read-only
            b) rw: Mounts as read-write
            c) user: Allows an ordinary user to mount the filesystem
            d) check=none: Mounts the fi lesystem without performing an integrity check
            e) loop: Mounts a file

C. To remove a removable media device, you should never just remove it from the system. Instead, you should always unmount it first
    1. The command used to unmount devices is umount
        a) umount [directory | device]
    2. If any program has a file open on a device, the system won't let you unmount it

VII. The df command allows you to easily see what's happening on all the mounted disks
A. The command displays the following:
    1. The device location of the device
    2. How many 1024-byte blocks of data it can hold
    3. How many 1024-byte blocks are used
    4. How many 1024-byte blocks are available
    5. The amount of used space as a percentage
    6. The mount point where the device is mounted
B. The -h parameter shows the disk space in human-readable form, usually as an M for megabytes or a G for gigabytes

VIII. The du command shows the disk usage for a specific directory
A. By default, the command displays all the files, directories, and subdirectories under the current directory and it shows how many disk blocks each file or directory takes
B. Parameters:
    1. -c: Produces a grand total of all the files listed
    2. -h: Prints sizes in human-readable form, using K for kilobyte, M for megabyte, and G for gigabyte
    3. -s: Summarizes each argument

IX. The sort command sorts data
A. By default, the command sorts the data lines in a text file using standard sorting rules for the language you specify as the default for the session
B. By default, the sort command interprets numbers as characters and performs a standard character sort, producing output that might not be what you want
    1. To solve this problem, use the -n parameter, which tells the sort command to recognize numbers as numbers instead of characters and to sort them based on their numerical values

C. If you use the -M parameter, the sort command recognizes the three-character month nomenclature and sorts appropriately
D. Use the -t parameter to specify the field separator character, and use the -k parameter to specify which field to sort on
E. The -r option also sorts the values in descending order, so you can easily see what files are taking up the most space in your directory

X. The grep command searches either the input or the file you specify for lines that contain characters that match the specified pattern
   A. grep [options] pattern [file]
   B. The output from grep is the lines that contain the matching pattern
   C. Parameters:
      1. -v: Reverse the search (output lines that don't match the pattern)
      2. -n: Find the line numbers where the matching patterns are found
      3. -c: Count of how many lines contain the matching pattern
      4. If you need to specify more than one matching pattern, use the -e parameter to specify each individual pattern
   D. The egrep command is an offshoot of grep, which allows you to specify POSIX extended regular expressions, which contain more characters for specifying the matching pattern
   E. The fgrep command is another version that allows you to specify matching patterns as a list of fixed-string values, separated by newline characters

XI. The zip utility allows you to easily compress large files (both text and executable) into smaller files that take up less space
   A. The gzip utility is the most popular compression tool used in Linux
      1. Package includes:
         a) gzip for compressing files
            (1) You can specify more than one filename or even use wildcard characters to compress multiple files at once
         b) gzcat for displaying the contents of compressed text files
         c) gunzip for uncompressing files

XII. By far the most popular archiving tool used in Unix and Linux is the tar command
   A. tar function [options] object1 object2 ...
   B. Was originally used to write files to a tape device for archiving
   C. Functions:

1. -A: Appends an existing tar archive file to another existing tar archive file
2. -c: Creates a new tar archive file
3. -d: Checks the differences between a tar archive file and the filesystem
4. -r: Appends files to the end of an existing tar archive file
5. -t: Lists the contents of an existing tar archive file
6. -u: Appends files to an existing tar archive file that are newer than a file with the same name in the existing archive
7. -x: Extracts files from an existing archive file

D. Options:

1. -C dir: Changes to the specified directory
2. f file: Outputs results to file (or device) file
3. -j: Redirects output to the bzip2 command for compression
4. -p: Preserves all file permissions
5. -v: Lists files as they are processed
6. -z: Redirects the output to the gzip command for compression