Vikash Kumar Deo

N15708475

Vkd225

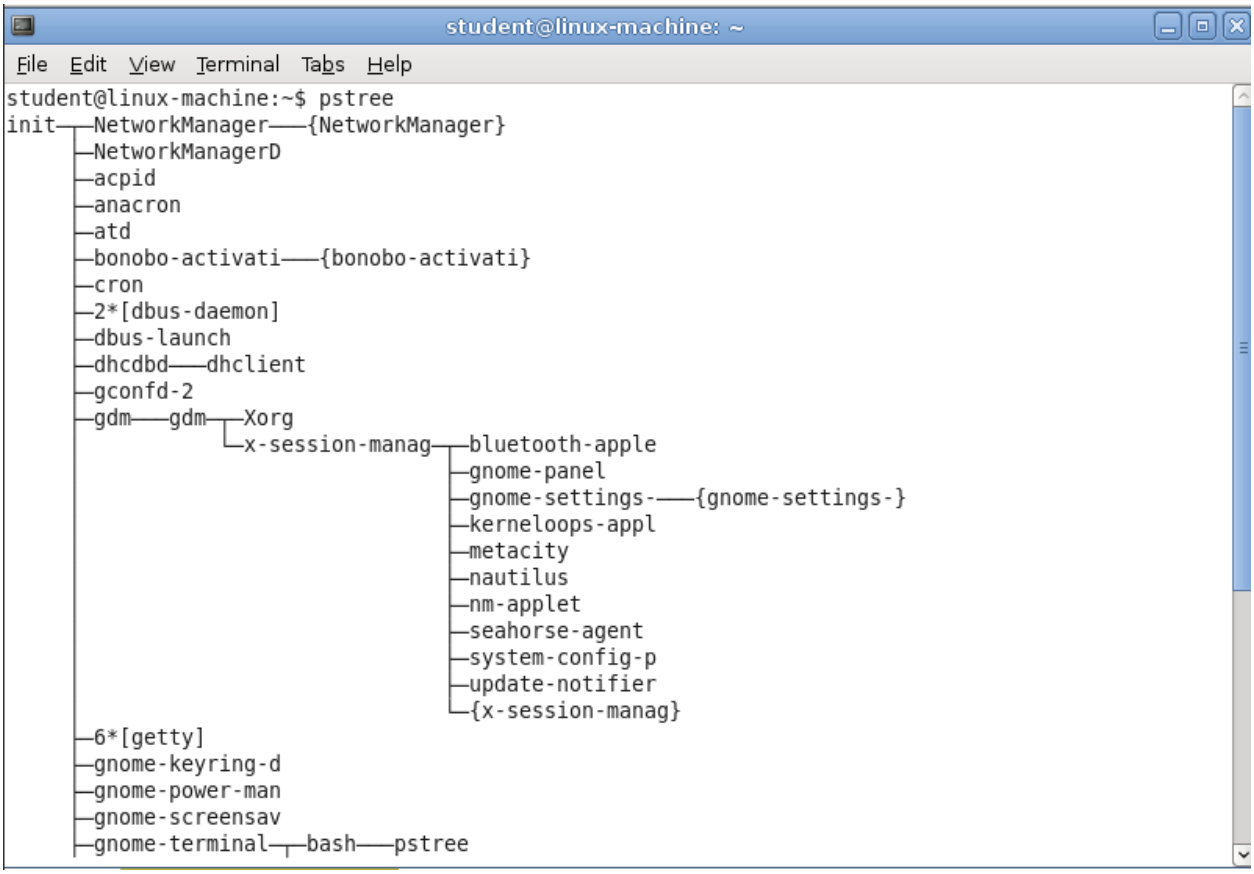
Network Security (CS 6823)

Lab -1

Due: 09/15/2015

1. “init” (short for initialization) is the first process that starts when a Linux Kernel starts. We can see that using ‘pstree’ which gives us a tree of the how and which process starts when the Kernel starts and is parent process of all the process.

The first processes that init starts is a script /etc/rc.d/rc.sysinit



2. The startup procedures of Linux box are

BIOS – Basic Input Output System
It performs startup assignments which is needed for the hardware platform and loads and executes the boot loader program. Once the hardware is set up and initialized properly, the BIOS performs integrity checks on memory and loads and executes the boot code from the configured boot device.

MBR – Master Boot Record
MBR is a special type of boot sector at the very beginning of partitioned computer mass storage devices like fixed disks or removable drives. This MBR code is usually referred to as a boot loader and points to the boot loader (GRUB or LILO: Linux boot loader).

GRUB – Grand Unified Bootloader

GRUB asks for the OS label which identifies which kernel to run and where it is located in system. The installation process require creation or identification of partitions and where to install the OS. GRUB are also configured during the process and then boot loader loads the OS. It also allows us to have multiple kernel images installed on our system, we can choose which one to be executed.

Kernel
Kernel which decompresses itself and sets up system functions such as essential hardware and memory paging, before calling start_kernel(). Kernel executes the /sbin/init program and since init is the 1st program to be executed by Linux Kernel, it has the process id (PID) of 1. Do a 'ps -ef | grep init' and check the pid.

Init (Initilization)
init looks at inittab file to linux run levels. (0- halt; 1- single user mode; 2- multiuser; 3- Full ultiuser mode; etc) init identifies this level to load appropriate program. The first thing the kernel does is to execute init program. Init is the root/parent of all processes executing on Linux.

Runlevel
When linux system is booting up, many runlevel programs get executed from run level directory as defined. These programs are generally run many executables like daemon processes, hardware abstraction layer, networking layer, dhcp etc.

Based on the appropriate run-level, scripts are executed to start various processes to run the system and make it functional.

3. Command used is : **grep –H –r –w "Hello CS6823" /etc**

```
linux-machine:/# grep -H -r -w "Hello CS6823" /etc
/etc/findme.txt:Hello CS6823!
linux-machine:/#
```

4. “ ps ” is a command that is used to see the running processes on system.

```
student@linux-machine:~$ ps
  PID TTY          TIME CMD
 2664 pts/0    00:00:00 bash
 2677 pts/0    00:00:00 ps
student@linux-machine:~$ ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0  10312   748 ?        Ss   19:34   0:05 init [2]
root         2  0.0  0.0      0     0 ?        S<   19:34   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   19:34   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   19:34   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   19:34   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   19:34   0:00 [migration/1]
root         7  0.0  0.0      0     0 ?        S<   19:34   0:00 [ksoftirqd/1]
root         8  0.0  0.0      0     0 ?        S<   19:34   0:00 [watchdog/1]
root         9  0.0  0.0      0     0 ?        S<   19:34   0:00 [events/0]
root        10  0.0  0.0      0     0 ?        S<   19:34   0:00 [events/1]
root        11  0.0  0.0      0     0 ?        S<   19:34   0:00 [khelper]
root        46  0.0  0.0      0     0 ?        S<   19:34   0:00 [kblockd/0]
root        47  0.0  0.0      0     0 ?        S<   19:34   0:00 [kblockd/1]
root        49  0.0  0.0      0     0 ?        S<   19:34   0:00 [kacpid]
root        50  0.0  0.0      0     0 ?        S<   19:34   0:00 [kacpi_notify]
root       107  0.0  0.0      0     0 ?        S<   19:34   0:00 [ksuspend_usbd]
root       113  0.0  0.0      0     0 ?        S<   19:34   0:00 [khubd]
root       116  0.0  0.0      0     0 ?        S<   19:34   0:00 [kseriod]
root       163  0.0  0.0      0     0 ?        S    19:34   0:00 [pdflush]
root       164  0.0  0.0      0     0 ?        S    19:34   0:00 [pdflush]
root       165  0.0  0.0      0     0 ?        S<   19:34   0:02 [kswapd0]
root       166  0.0  0.0      0     0 ?        S<   19:34   0:00 [aio/0]
root       167  0.0  0.0      0     0 ?        S<   19:34   0:00 [aio/1]
```

“Ps ux” is the command to see all the process running on the system of user “student”.

```
student@linux-machine:~$ ps ux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
student   2256  0.0  0.4  40804  4964 ?        S    19:34   0:00 /usr/lib/libgconf2-4/gconfd-2 11
student   2258  0.0  0.2  58868  2328 ?        S    19:34   0:00 /usr/bin/gnome-keyring-daemon -d
student   2259  0.0  0.7 188912  7956 ?        Ssl  19:34   0:00 x-session-manager
student   2307  0.0  0.0  25732   728 ?        S    19:34   0:00 /usr/bin/dbus-launch --exit-with
student   2308  0.0  0.0  21220   992 ?        Ss   19:34   0:00 /usr/bin/dbus-daemon --fork --pr
student   2314  0.0  0.8 219368  8648 ?        Ss   19:34   0:00 /usr/bin/seahorse-agent --execut
student   2317  0.0  1.1 254212 11280 ?        Sl   19:34   0:00 gnome-settings-daemon
student   2334  0.0  1.2 133496 13048 ?        S    19:35   0:01 /usr/bin/metacity --sm-client-id
student   2337  0.0  2.0 285608 20856 ?        S    19:35   0:03 gnome-panel --sm-client-id defau
student   2338  0.0  3.0 443056 30768 ?        S    19:35   0:07 nautilus --no-default-window --s
student   2344  0.0  0.3 147636  3640 ?        Ssl  19:35   0:00 /usr/lib/bonobo-activation/bonob
student   2345  0.0  0.5 139164  6004 ?        Ss   19:35   0:01 gnome-screensaver
student   2347  0.0  0.6 124844  6240 ?        S    19:35   0:00 bluetooth-applet --singleton
student   2350  0.0  0.4  90144  4428 ?        S    19:35   0:00 /usr/lib/gnome-vfs-2.0/gnome-vfs
student   2351  0.0  1.5 209236 15820 ?        S    19:35   0:01 update-notifier
student   2360  0.0  1.6 207360 16584 ?        S    19:35   0:00 /usr/bin/python /usr/bin/system-
student   2362  0.0  0.5 115660  5464 ?        S    19:35   0:00 kerneloops-applet
student   2363  0.0  0.5 181728  5424 ?        Ss   19:35   0:00 /usr/lib/gnome-volume-manager/gn
student   2364  0.0  1.2 193836 13176 ?        S    19:35   0:03 nm-applet --sm-disable
student   2365  0.0  0.8 205556  8380 ?        Ss   19:35   0:00 gnome-power-manager
student   2377  0.0  1.5 217204 16160 ?        S    19:35   0:00 /usr/lib/gnome-applets/mixer_app
student   2383  0.0  0.0  17244  1000 ?        S    19:35   0:00 /usr/lib/nautilus-cd-burner/mapp
student   2660  0.1  1.5 225108 16252 ?        Rl   22:34   0:00 gnome-terminal
student   2663  0.0  0.0  19292   828 ?        S    22:34   0:00 gnome-pty-helper
student   2664  0.0  0.3  20480  3376 pts/0    Ss   22:34   0:00 bash
student   2711  0.0  0.1  16012  1100 pts/0    R+   22:40   0:00 ps ux
student@linux-machine:~$
```

“**Kill**“is the command to kill the process.

5. Setup variables are declared with the echo command, or simply by setting them equal to something. For example, echo a=123 creates a variable named "a" containing the value "123". Unlike variables in some other languages, a type is not necessary; the values are stored as strings. To remove them without logging out we use the unset command.

```
linux-machine:/# echo a=1
a=1
linux-machine:/# echo a=123
a=123
linux-machine:/# unset a
linux-machine:/# echo a
a
linux-machine:/#
```

6. We can use last “**last bootup** “to see when the system was last booted up.

```
linux-machine:/# last bootup

wtmp begins Mon Sep 14 21:09:44 2015
linux-machine:/#
```

7. In all UNIX based systems, a UID, or "user ID number", is an integer that identifies a particular user. Every running process has at least two UID numbers associated with it, the real UID number, which identifies the user who launched the process, and the effective UID number, which is used to determine what resources the process can access.

Effective user-ID is that of the user who owns the file. It is used particularly for checking whether process can open a file or not i.e. ownership accesses are managed by effective user-id. The effective ID is the ID that the system uses to determine whether a process can take a particular action.

Normally these are the same, but if a program with a set-uid bit set is run, then while the real UID remains that of the user who ran it, the effective UID is that of the user who owns the file.

1.1 Linux Commands

1.

File and Directory Management: grep, find, ls, chmod, chown, rmdir, whereis, ln, rm, cp, mv, ld, tar, df, patch, mkdir

Communication: ssh, sftp, ftp

User Management: passwd, useradd, adduser, su, last

Editing: man, vi, more, cat, less

Process Management: lsmod, make, ps, kill

Misc. Commands: | (pipe), >, >> (output redirection), < (input redirection), top, fdisk and cfdisk: fdisk, insmod

2.

Grep - Search file(s) for lines that match a given pattern.
SYNTAX grep [options] PATTERN [FILE...]
grep [options] [-e PATTERN | -f FILE] [FILE...]
Options
Export Option:
export GREP_OPTIONS='—color=auto' GREP_COLOR='100;8'
Find files using grep:
find . -name "*.txt" | xargs grep "stuff"
N lines after, before and around the grep match (respectively):
grep -A <N> "stuff" FILE
grep -B <N> "stuff" FILE
grep -C <N> "stuff" FILE
Counting using grep (count, count recursively, count inverse):
grep -c "stuff" FILENAME
grep -rc "stuff" .
grep -rvc "stuff" .

Display only file names (+ recursively):
grep -l "stuff" *.log
grep -rl "stuff" .
Watching console output with grep:
tail -f FILENAME | grep "stuff"
Commonly used grep options:
-a = for binary files
-h = suppress the file names
-i = ignore cases
-l = file names only

Find - Search for files that meet a desired criteria.
SYNTAX find [-H] [-L] [-P] [path...] [expression]
Options
All options always return true. Except for -follow and -daystart, they always take effect, rather than being processed only when their place in the expression is reached. Therefore, for clarity, it is best to place them at the beginning of the expression. A warning is issued if you don't do this.
-daystart
Measure times (for -amin, -atime, -cmin, -ctime, -mmin, and -mtime) from the beginning of today rather than from 24 hours ago. This option only affects tests which appear later on the command line.
-depth
Process each directory's contents before the directory itself.
-d
A synonym for -depth, for compatibility with FreeBSD, NetBSD, MacOS X and OpenBSD.
-follow
Deprecated; use the -L option instead. Dereference symbolic links. Implies -noleaf. The -follow option affects only those tests which appear after it on the command line. Unless the -H or -L option has been specified, the position of the -follow option changes the behaviour of the -newer predicate; any files listed as the argument of -newer will be dereferenced if they are symbolic links. The same consideration applies to -anewer and -cnewer. Similarly, the -type predicate will always match against the type of the file that a symbolic link points to rather than the link itself. Using -follow causes the -lname and -ilname predicates always to return false.
-help, --help
Print a summary of the command-line usage of find and exit.
-ignore_readdir_race
Normally, find will emit an error message when it fails to stat a file. If you give this option and a file is deleted between the time findreads the name of the file from the directory and the time it tries to stat the file, no error message will be issued. This also applies to files or directories whose names are given on the command line. This option takes effect at the time the command line is read, which means that you cannot search one part of the filesystem with this option on and part of it with this option off (if you need to do that, you will need to issue two find commands instead, one with the option and one without it).
-maxdepth levels
Descend at most levels (a non-negative integer) levels of directories below the command line arguments. '-maxdepth 0' means only apply the tests and actions to the command line arguments.
-mindepth levels
Do not apply any tests or actions at levels less than levels (a non-negative integer). '-mindepth 1' means process all files except the command line arguments.
-mount
Don't descend directories on other filesystems. An alternate name for -xdev, for compatibility with some other versions of find.
-noignore_readdir_race
Turns off the effect of -ignore_readdir_race.
-noleaf

Do not optimize by assuming that directories contain 2 fewer subdirectories than their hard link count. This option is needed when searching filesystems that do not follow the Unix directory-link convention, such as CD-ROM or MS-DOS filesystems or AFS volume mount points. Each directory on a normal Unix filesystem has at least 2 hard links: its name and its '.' entry. Additionally, its subdirectories (if any) each

have a '..' entry linked to that directory. When find is examining a directory, after it has statted 2 fewer subdirectories than the directory's link count, it knows that the rest of the entries in the directory are non-directories ('leaf' files in the directory tree). If only the files' names need to be examined, there is no need to stat them; this gives a significant increase in search speed.

-regextype type
Changes the regular expression syntax understood by -regex and -iregex tests which occur later on the command line. Currently-implemented types are emacs (this is the default), posix-awk, posix-basic, posix-egrep and posix-extended.
-version, --version
Print the find version number and exit.
-warn, -nowarn
Turn warning messages on or off. These warnings apply only to the command line usage, not to any conditions that find might encounter when it searches directories. The default behaviour corresponds to -warn if standard input is a tty, and to -nowarn otherwise.
-xdev
Don't descend directories on other filesystems.

Ls – This command lists information about files.
SYNTAX ls [Options]... [File]...
Options
The most common options are -a (all files) and -l (long or details)

Rmdir – This command is used to remove directories. It will only work when the directories are empty.
SYNTAX rmdir [options]... folder(s)...
Options
--ignore-fail-on-non-empty
Ignore each failure that is solely because the directory is non-empty.
-p, --parents Remove explicit parent directories if being emptied
--verbose Output a diagnostic for every directory processed
--help Display help and exit
--version Output version information and exit

Whereis - Search $path, man pages and source files for an application file.
The supplied filenames are first stripped of leading pathname components and any (single) trailing extension of the form .ext (for example, .c). Prefixes of s. resulting from use of source code control are also dealt with. whereis then attempts to locate the desired program in a list of standard Linux directories (e.g., /bin, /etc, /usr/bin, /usr/local/bin/, etc.).
SYNTAX whereis [options] files
Options
-b Search only for binaries.
-B directories
Change or otherwise limit the directories to search for binaries.
-f Terminate the last directory list and signal the start of filenames; Required when any of the -B, -M, or -S options are used.
-m Search only for manual sections.
-M directory

Change or otherwise limit the directories to search for manual sections.
-s Search only for sources.
-S directory
Change or otherwise limit the directories to search for sources.
-u Search for unusual entries, that is, files that do not have one entry of each requested type. Thus, the command whereis -m -u * asks for those files in the current directory that have no documentation.

Fdisk – It manipulates the partition table in linux.
SYNTAX fdisk [-u] device
fdisk -l [-u] device ...
fdisk -s partition ...
fdisk –v

Options
-u When listing partition tables, give sizes in sectors instead of cylinders.
-l List the partition tables for /dev/hd[a-d], /dev/sd[a-h], /dev/ed[a-d], and then exit.
-s partition
The size of the partition (in blocks) is printed on the standard output.
-v Print version number of fdisk program and exit.

Ln – Used to make links between files, by default, it makes hard links; with the `-s' option, it makes symbolic (or "soft") links.
SYNTAX ln [Options]... target [Linkname]
ln [Options]... target... Directory
Options
-b
--backup
Make a backup of each file that would otherwise be overwritten or
removed. *Note Backup options::.
-d
-F
--directory
Allow the super-user to make hard links to directories.
-f
--force
Remove existing destination files.
-i
--interactive
Prompt whether to remove existing destination files.
-n
--no-dereference
When given an explicit destination that is a symlink to a directory, treat that destination as if it were a normal file.
-s
--symbolic
Make symbolic links instead of hard links. This option merely
produces an error message on systems that do not support symbolic

links.
-S SUFFIX
--suffix=SUFFIX
Append SUFFIX to each backup file made with `-b'. *Note Backup
options::.
-v
--verbose
Print the name of each file before linking it.
-V METHOD
--version-control=METHOD
Change the type of backups made with `-b'. The METHOD argument
can be `numbered' (or `t'), `existing' (or `nil'), or `never' (or
`simple').

Rm – This command is used to remove/delete files.
SYNTAX rm [options]... file...
Options
-d, --directory unlink directory, even if non-empty (super-user only)
-f, --force ignore nonexistent files, never prompt
-i, --interactive prompt before any removal
-r, -R, --recursive remove the contents of directories recursively
-v, --verbose explain what is being done
--help display this help and exit
--version output version information and exit
To remove a file we must have write permission on the file and the folder where it is stored.

Cp – This command is used to copy one or more files to another location or copy SOURCE to DEST, or multiple SOURCE(s) to DIRECTORY.
SYNTAX cp [options]... Source Dest
cp [options]... Source... Directory
Options
-a, --archive same as -dpR
-b, --backup make backup before removal
-d, --no-dereference preserve links
-f, --force remove existing destinations, never prompt
-i, --interactive prompt before overwrite
-l, --link link files instead of copying
-p, --preserve preserve file attributes if possible
-P, --parents append source path to DIRECTORY
-r copy recursively, non-directories as files
--sparse=WHEN control creation of sparse files
-R, --recursive copy directories recursively
-s, --symbolic-link make symbolic links instead of copying
-S, --suffix=SUFFIX override the usual backup suffix
-u, --update copy only when the SOURCE file is newer than the destination file or when the destination file is missing

-v, --verbose explain what is being done
-V, --version-control=WORD override the usual version control
-x, --one-file-system stay on this file system
--help display this help and exit
--version output version information and exit.

Mv – This command is used to move or rename files or directories.
SYNTAX mv [options]... Source Dest
mv [options]... Source... Directory
If the last argument names an existing directory, `mv' moves each other given file into a file with the same name in that directory. Otherwise, if only two files are given, it renames the first as the second. It is an error if the last argument is not a directory and more than two files are given.
Options
-b
--backup
Make a backup of each file that would otherwise be overwritten or
removed.
-f
--force
Remove existing destination files and never prompt the user.
-i
--interactive
Prompt whether to overwrite each existing destination file,
regardless of its permissions. If the response does not begin
with `y' or `Y', the file is skipped.
-S SUFFIX
--suffix=SUFFIX
Append SUFFIX to each backup file made with `-b'.
The backup suffix is ~, unless set with SIMPLE_BACKUP_SUFFIX.
-u
--update
Do not move a nondirectory that has an existing destination with
the same or newer modification time.
-v
--verbose
Print the name of each file before moving it.
-V METHOD
--version-control=METHOD'
Change the type of backups made with `-b'. METHOD can be:
t, numbered make numbered backups
nil, existing numbered if numbered backups exist, simple otherwise
never, simple always make simple backups
--help display help and exit
--version output version information and exit

Cat – This command is used to concatenate and print (display) the content of files.
SYNTAX cat [Options] [File]...
Concatenate FILE(s), or standard input, to standard output.
-A, --show-all equivalent to -vET
-b, --number-nonblank number nonblank output lines
-e equivalent to -vE
-E, --show-ends display $ at end of each line
-n, --number number all output lines
-s, --squeeze-blank never more than one single blank line
-t equivalent to -vT
-T, --show-tabs display TAB characters as ^I
-u (ignored) or list from an archive may be given as shell pattern matching strings.

Options
-C, --directory DIR
-f, --file F
-j, --bzip2
-p, --preserve-permissions
-v, --verbose
-z, --gzip

Df - Disk Free - display free disk space. With no arguments, `df' reports the space used and available on all currently mounted file systems (of all types). Otherwise, `df' reports on the file system containing each argument file.
SYNTAX df [option]... [file]...
Options
-a, --all
include dummy file systems
-B, --block-size=SIZE use SIZE-byte blocks
-h, --human-readable
print sizes in human readable format

Patch - This command is used to apply a diff file to the original. patch takes a patch file patchfile containing a difference listing produced by the diff program and applies those differences to one or more original files, producing patched versions.

Mkdir - Create new folder(s), if they do not already exist.
SYNTAX mkdir [Options] folder...
mkdir "Name with spaces"
Options
-m, --mode=MODE set permission mode (as in chmod), not rwxrwxrwx - umask
-p, --parents no error if existing, make parent directories as needed
--verbose print a message for each created directory

Chmod - Change access permissions, change mode.
SYNTAX chmod [Options]... Mode [,Mode]... file...
chmod [Options]... Numeric_Mode file...
chmod [Options]... --reference=RFile file...
Options
-f, --silent, --quiet suppress most error messages
-v, --verbose output a diagnostic for every file processed
-c, --changes like verbose but report only when a change is made
--reference=RFile use RFile's mode instead of MODE values
-R, --recursive change files and directories recursively
--help display help and exit
--version output version information and exit

Chown - nChange owner, change the user and/or group ownership of each given File to a new Owner. Chown can also change the ownership of a file to match the user/group of an existing reference file.
SYNTAX chown [Options]... NewOwner File...
chown [Options]... :Group File...
chown [Options]... --reference=RFILE File...
If used, NewOwner specifies the new owner and/or group as follows
(with no embedded white space):
[OWNER] [[:.] [GROUP]]
Options
-c
--changes
Verbosely describe the action for each FILE whose ownership actually changes.
--dereference
Do not act on symbolic links themselves but rather on what they point to.
-f
--silent
--quiet
Do not print error messages about files whose ownership cannot be changed.
-h
--no-dereference
Act on symbolic links themselves instead of what they point to. This is the default. This mode relies on the `lchown' system call. On systems that do not provide the `lchown' system call, `chown' fails when a file specified on the command line is a symbolic link.
--reference=FILE
Use the user and group of the reference FILE instead of an explicit NewOwner value.
-R
--recursive
Recursively change ownership of directories and their contents.
-v
--verbose
Verbosely describe the action (or non-action) taken for every FILE.

Passwd - Modify a user password.
SYNTAX passwd [options...]
OPTIONS
-d, --delete delete the password for the named account (root only)
-f, --force force operation (effectively calls `chfn'?)
-k, --keep-tokens keep non-expired authentication tokens
-l, --lock lock the named account (root only)
-S, --status report password status on the named account (root only)
--stdin read new tokens from stdin (root only)
-u, --unlock unlock the named account (root only)
--usage Display brief usage message
If no options are specified - passwd will change the password of the currently logged in user - will prompt for the old and new passwords.

Useradd - Create a new user or update default new user information .
SYNTAX useradd [options] LOGIN
useradd -D
useradd -D [options]
Options
-b The default base directory for the system if –d HOME_DIR is not specified.
-c It is used for comment which can be any text string. This is currently used as user's full name.
Adduser has same function as Useradd but differs in its implementation for different Distributions

Su - Substitute user identity. Run a command with substitute user and group id, allow one user to temporarily become another user. It runs a command (often an interactive shell) with the real and effective user id, group id, and supplemental groups of a given user.
SYNTAX su [options]... [user [arg]...]
Options
-c COMMAND
--command=COMMAND
Pass COMMAND, a single command line to run, to the shell with a
-c option instead of starting an interactive shell.
-f
--fast
Pass the `-f' option to the shell. This probably only makes senseif the shell run is `csh' or `tcsh', for which the `-f' option prevents reading the startup file (`.cshrc'). With Bourne-like shells, the `-f' option disables file name pattern expansion (globbing), which is not likely to be useful.
-
-l
--login
Make the shell a login shell. This means the following. Unset all environment variables except `TERM', `HOME', and `SHELL' (which are set as described above), and `USER' and `LOGNAME' (which are set, even for the super-user, as described above), and set `PATH' to a compiled-in default value. Change to USER's home directory. Prepend `-' to the shell's name, intended to make it read its login startup

file(s).
-m
-p
--preserve-environment
Do not change the environment variables `HOME', `USER', `LOGNAME', or `SHELL'. Run the shell given in the environment variable `SHELL' instead of the shell from USER's passwd entry, unless the user running `su' is not the superuser and USER's shell is restricted. A "restricted shell" is one that is not listed in the file `/etc/shells', or in a compiled-in list if that file does not exist. Parts of what this option does can be overridden by `--login' and `--shell'.
-s SHELL
--shell=SHELL
Run SHELL instead of the shell from USER's passwd entry, unless the user running `su' is not the superuser and USER's shell is restricted

Last – This command is used to list the last logged in users.

Lsmod – It's a command to show the status of modules in the Linux Kernel.
SYNTAX lsmod [-hV]

Insmod - This command installs a loadable module in the running kernel. It tries to link a module into the running kernel by resolving all symbols from the kernels exported symbol table.
Options
-e Specifies where any persistent data for the module is read from on load and written to when the instantiation of the module is unloaded.
-L is used to prevent simultaneous loads of same module.

Make - It's a command used to recompile a group of programs.
Options
-b These options are ignored for compatibility with other versions of make.
-B Unconditionally make all targets.

Ps - Process status, information about processes running in memory. If you want a repetitive update of this status, use top.
SYNTAX
ps option(s)
ps [-L]
Options
-L List all the keyword options

Kill - Stop a process from running, either via a signal or forced termination.
SYNTAX kill [-s sigspec] [-n signum] [-sigspec] jobspec or pid
kill -l [exit_status]
kill -l [sigspec]
Key
-l List the signal names

-s Send a specific signal
-n Send a specific signal number

Ssh – OpenSSH SSH client (remote login program).
SYNTAX
ssh [-1246AaCfgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
[-D [bind_address:]port] [-e escape_char] [-F configfile]
[-i identity_file] [-L [bind_address:]port:host:hostport]
[-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option]
[-p port] [-R [bind_address:]port:host:hostport]
[-S ctl_path] [-w local_tun[:remote_tun]]
[user@]hostname [command]
Options
-1 Forces ssh to try protocol version 1 only.
-2 Forces ssh to try protocol version 2 only.
-4 Forces ssh to use IPv4 addresses only.
-6 Forces ssh to use IPv6 addresses only.

ftp - It is internet file transfer protocol. The program allows user to transfer files to and from a remote server.
Options
-p uses passive mode for file transfers.
-A uses active mode for data transfers.

Sftp - It is an interactive file transfer program which performs all operations over an encrypted ssh channel.
Options
-B Specify the buffer size that sftp uses when transferring files.
-C Enables Compression.

Pipe - Pipe creates a unidirectional data channel that can be used for and interprocess communication channel. A pipe has a read end and a write end. Data written in the write end can be read from the read end.

Redirection - Redirection simply means capturing output from a file, command, program, script, or even code block within a script and sending it as input to another file, command, program, or script.
> It redirects output from file descriptor n to a file. If the file exists the existing contents are lost without any warning.
>> It redirects output from file descriptor n to a file. If the file exists the new contents are appended at the end of the file.

Vi - Vi is an text editor. Vi operates in two modes insert mode and command mode.
SYNTAX vi [filename]
Start vi Use following command vi filename.
Quit vi Enter command mode and use :wq to save the contents and quit

More - Display output one screen at a time, less provides more emulation and extensive enhancements.
SYNTAX more [-dlfpcsu] [-num] [+/ pattern] [+ linenum] [file ...]
Options
-num This option specifies an integer which is the screen size (in lines).
-d more will prompt the user with the message "[Press space to continue,'q' to quit.]" and will display "[Press 'h' for instructions.]"instead of ringing the bell when an illegal key is pressed.
-l more usually treats ^L (form feed) as a special character, and will pause after any line that contains a form feed. The -l option will prevent this behavior.
-f Causes more to count logical, rather than screen lines (i.e., long lines are not folded).
-p Do not scroll. Instead, clear the whole screen and then display the text.
-c Do not scroll. Instead, paint each screen from the top, clearing the remainder of each line as it is displayed.
-s Squeeze multiple blank lines into one.
-u Suppress underlining.
+/ The +/ option specifies a string that will be searched for before each file is displayed.
+num Start at line number num

Less – Less is a program similar to more, but which allows backward movement in the file as well as forward movement. Also, less does not have to read the entire input file before starting, so with large input files it starts up faster than text editors like vi.

Man - Format and display help pages.
SYNTAX
man [-acdfFhkKtwW] [--path] [-m system] [-p string] [-C config_file]
[-M pathlist] [-P pager] [-B browser] [-H htmlpager] [-S section_list]
[section] name ...

Top - Process viewer, find the CPU-intensive programs currently running. See ps for explanations of the field descriptors.
SYNTAX top *options*

Options
-b Run in batch mode; don't accept command-line input.
Useful for sending output to another command or to a file.
-c Show command line in display instead of just command name.
-d delay
Specify delay between refreshes.
-i Suppress display of idle and zombie processes.
-n num
Update display num times, then exit.
-p pid
Monitor only processes with the specified process ID.
-q Refresh without any delay.
If user is privileged, run with highest priority.
-s Secure mode. Disable some (dangerous) interactive commands.
-S Cumulative mode. Print total CPU time of each process,
including dead child processes

References:

Master boot record - Wikipedia, the free encyclopedia - en.wikipedia.org

Linux: Init Process and PC Boot Procedure - www.yolinux.com

Linux startup process - Wikipedia, the free encyclopedia - en.wikipedia.org

Finding a File Containing a Particular Text String In Linux Server - www.cyberciti.biz