**Key Commands**

**General Commands**

* `ls` List all the items in a directory
* `cd` Change directory
* `mv` Move a file
* `cp` Copy a file
* `less` Read a file with pagination
* `head` View the top 10 lines of a file
* `tail` View the bottom 10 lines of a file
* `>` Redirect the output of a command into a file
* `mkdir` Create a directory
* `rm` Remove a file or a directory
* `whoami` Display the current user name
* `groups` Display the groups for a user
* `man` Open the manual for a command

**ls -l**

List the 'long' form of files and directories in your present working directory.

#List 'all' the files in 'long' form with 'human' readable file sizes.

ls -alh

This is used to see the permissions of files/directories, the username and group of the file/directory owner, the file/directory size in bytes and the time of it's last modification.

**Kill and Killall**

Kill is used for killing a process using the process ID. Killall is used to kill *all* the processes started by the same program. Killall uses the process name.

#Kill process with the ID 436

kill 436

#Kill all processes started by the chrome program

killall chrome

By default kill allows the process to stop what it's doing and wrap things up before is stops. If you want to 'pull the plug' on a program and kill it immediately, use the -9 option.

# kill process with the id 567 immediately

kill -9 567

**Apt-get and Apt**

Apt-get is the standard command to install packages on all Debian based systems. apt is a shorthand version that works the same way. If you want the package to be installed without out further questioning from the system, you can use the -y flag

# Install the nano package

sudo apt-get install nano

# Install the top package without asking for confirmation

sudo apt-get -y install top

**Nano and text editors**

Nano is a basic text editor in Linux. There are other text editors listed here as well for you to try. If you decide to try these, google them first to learn about how they work. The man pages are also a good resource.

# open my\_doc.txt with the nano text editor

nano my\_doc.txt

# open my\_doc.txt with the gedit text editor

gedit my\_doc.txt

# open my\_doc.txt with the vi text editor

vi my\_doc.txt

# open my\_doc.txt with the emacs text editor

emacs my\_doc.txt

**sudo**

Stands for 'Super User Do'. It's the command you have to use if you want to invoke the system permissions of the root user (also known as the super user).

# Show the contents of the /etc/shadow file

sudo cat /etc/shadow

# Update the list of programs offered in the `apt` repository

sudo apt update

Many files/directories are only accessible by the root user. Also many programs require root permissions to run. If you are not logged in as root, you either have to switch your login to the root user, or you can use sudo command to run a single command with root permissions. Note: In order to use the 'sudo' command, your user has to be part of the 'sudo' group.

You can see what commands are available for your user with the -l flag

# Print the available sudo commands for the current user

sudo -l

If you want to see what commands are available for another user, add the -U flag and the username

# Print the available sudo commands for the user mike

sudo -lU mike

**su**

Stands for 'Switch User'. If you do not specify a user to switch to, the default is root.

# Switch to user mike

su mike

# Switch your login to the root user and 'preserve' your current environment.

su -p

**visudo**

You *must* use visudo to edit the /etc/sudoers file.

# Edit the /etc/sudoers file and validate that it is not damaged before saving.

sudo visudo -c

**chage**

Chage allows an administrator to set expirations on passwords, along with setting how many days before the next password change.

To see all of the chage info for a user, use the -l flag

# look at the chage info for the user mike

sudo chage -l mike

To set the Maximum number of days between password changes use the -M flag

# set the password to expire after 90 days for the user mike

chage -M 90 mike

To set the password to expire immediately, use the -d flag with the value 0

# set the password to expire immediately for the user mike

chage -d 0 mike

**id**

The id command gives you the UID, GID, and group information for a user.

#Show the UID, GID, and group information for user randal.

id randal

If no user is specified, the current user's info is displayed.

**adduser**

adduser makes it easy to add a user with their password and user info.

# Add a new user with the username 'ralph'

sudo adduser ralph

If you want to create a system user use the --system option to give the user a UID < 1000. Use the --no-create-home option to avoid creating a home folder.

# Create a system user named http without creating a home folder

sudo adduser --system --no-create-home http

**addgroup**

addgroup allows you to make and create groups on the system.

# Create a new group named 'developers'

addgroup developers

**usermod**

usermod allows you to change many parameters of a user. It is typically used to change a user's primary group, or add/remove secondary groups.

# Add the user bertha to the group hr\_administrators

usermod -aG hr\_administrates bertha

# Remove the user jack from all groups except the jack group

sudo usermod -G jack jack

**deluser**

deluser allows you to easily delete a user from the system. If you would like to also remove their home folder and files, use the --remove-home flag

# remove the user torbin from the system and delete his home folder

sudo deluser --remove-home torbin

**delgroup**

delgroup lets you easily remove a group from the system

# remove the slackers group from the system

sudo delgroup slackers

**chmod**

You change permissions with the command chmod, which stands for "change mode".

# Change the permissions to rwx for the user, rw- for the group and --- for everyone else.

chmod u+rwx,g=rw,o= permissions\_file

You can also use chmod with octal notation to set permissons.

# Change the permissions to rwx for the user, rw- for the group and --- for everyone else.

chmod 760 permissions\_file

**chown**

Stands for 'change owner'. When you change the owner, you also have to specify the group that you are assigning.

# Change the owner to bernard and the group to finance for the file spreadsheet

chown bernard:finance spreadsheet

Anything else about the Command

**Passwd**

The passwd command lets you change the password for a user.

#change the password for the user maxwell

sudo passwd maxwell

**Find**

Find is a great search tool to search for any files or folders on the system. To speicify between files or folders, user the -type flag along with f for files or d for directories.

# find all \_files\_ in the /etc directory

find /etc -type f

# find all \_directories\_ in the /etc directory

find /etc -type d

If you would like to search for a string in the name of the file, use the -iname flag along with the -type flag

# find a file with 'shadow' in the name inside the /etc directory

find /etc -iname shadow -type f

To search for files with particular permissions, use the -perm flag

# search for files that have the 2000 (SGID) bit set inside /usr/bin

find /usr/bin -perm /2000 -type f

# search for files that have the 4000 (SUID) bit set inside /usr/bin

find /usr/bin -perm /4000 -type f

**Systemctl**

systemctl allows you to start, stop, enable, disable and get the status of a service, as well as view all the services installed and running on the system. To get the status of a service use status and to see all the services, use -t for type along with service and --all to get everything on the system.

# search for \_all\_ services that are currently running on the system

systemctl -t service --all

# get the status of the apache2 service

sudo systemctl status apache2

If you want to start or stop a service, simply use start or stop flags

# start the apache2 service

sudo systemctl start apache2

# stop the apache2 service from running

sudo systemctl stop apache2

systemctl allows you to enable and disable a service from starting automatically when the system boots up. To set either of these, simply use enable or disable

# stop the apache2 service from starting automatically when the system starts up

sudo systemctl disable apache2

# set the apache2 service to start automatically when the system starts up

sudo systemctl enable apache2