*apt-get update* -download update

*apt-get upgrade* -install downloaded updates

*service --status-all* -all programs

*uname -a* -the os version

*ls -a* -list hidden files

*pwd* -print working directory

*rm -r <folder name>* -remove directory

*sudo -l*  -to become root

*sudo -s*  -to become root

*sudo su* -to become root

*exit* -to exit out of root

*less <file>* -writes content of file to screen (q to quit, space-bar for next page)

*head <file>* -first ten lines of file ( head -5 for just first 5)

*tail <file>* -last ten lines

*grep <file>* -searches file for word or pattern (-I to ignore case sensitivity)

*wc <file>* -word count(-l to get how many lines)

*ps* -list current processes

*kill <pid>* -kill process (kill -9 <pid> if a process refuses to be killed)

*whereis <option>* -bianary search

*which <option>*  -locates path of executable in path (ex which ls)

*whatis <option>* -brief information from man page

*find . <option>* -searches files for attributes given (ex find . -name “\*.txt” -print or find . -size +1M -ls)

*history* -history for command used (!! For last, !-3 for third most recent, !grep for commands starting with grep, or set history=100 to set size of buffer)

*tar xzf <file>* -extract .gz file to a file of same name

gunzip <file> -extract .gz file

*tar -xvf <file>* -extract .tar file

*make* -build packages (make check to see if everything compiled successfully)

*make install* -installs package (run from directory with ./)

*wget <link>* -download from link

*sudo apt-get --purge remove <program>* -removes program, --purge removes configs

*ps aux* -which processes are running

*sort –nk3 -t: /etc/passwd* -what users have been created recently

*sudo grep ALL /etc/sudoers* -Who has root

*netstat -nlp* -what ports are active

*systemctl | grep "^.\*\.service"* -what services are there

*journalctl | grep sudo* -what sudo commands have been run

* Adding users

*sudo visudo* -to add user to sudoers (need to add <name> ALL=ALL(ALL:ALL) ALL

*sudo userdel -r <name>*  -remove a user from system

*useradd [option] <name>* -create user account

*useradd -e {yyyy-mm-dd} {username}* -create account with disable date

*useradd -f {days} {username}* -set defauly passowrd expiry (0 to diable immediately after the password expires, -1 for account is not be diable after password expires)

* Adding group

*groupadd <groupname>*

*usermod -a -G <groupname> username* -adding a user to a group

*usermod -a -G admins <username>* -add a user to group admins

*usermod -g <groupname> username* -change a users primary group

*id <username>* -check permissions of a user

*groups* -list of groups

*useradd -g <groupname> username* -add a new user and assign a group

*/etc/init.d/<program>*  - containing the init program (the first process that is run when the kernel has finished initializing¹) as well as some infrastructure to start and stop services and configure them (can start, stop, restart, reload, status)

* Change hostname

*/etc/hostname*

*/etc/host*

* Files to check

*/etc/sudoers* -checking sudoers file

*/.bash\_history* -bash commands that have been run

*/etc/passwd* -registered users that has access to system

*/etc/shadow* -contains encrypted password as well as other information such as account or password expiration values

*/etc/sudoers -*use visudo to edit (contains the rules that users must follow when using the sudo command)

*/.bashrc* -shell script that Bash runs whenever it is started interactively

*/.shrc -*

*/.profile -*

*/var/spool/cron/crontabs -* Check crontabs (has list of commands you want to run regularly)

*Echo $PATH* - specifying a set of directories where executable programs are located

*less ~/.mysql\_history* -mysql history

Make sure /boot/grub/grub.cfg is owned by root:root

Check /temp

---------------------------------------------------------------------------------------------------------------------

* change access rights to a file

*chmod* ( u : user, g : group, o : other, a : all, r : read, w : write and delete, x : execute, + : add premession, - : takeaway permissions)

*chown* - change file ownership

*chgrp* - change a file's group owner

*ls -l* -check permissions on the file/users

ex: chmod go-rwx biglist (removes read,write, and exectute permission on file for group and others)

777 - (rwxrwxrwx) No restrictions on permissions. Anybody may do anything. Generally not a desirable setting.

755 - (rwxr-xr-x) The file's owner may read, write, and execute the file. All others may read and execute the file. This setting is common for programs that are used by all users.

700 - (rwx------) The file's owner may read, write, and execute the file. Nobody else has any rights. This setting is useful for programs that only the owner may use and must be kept private from others.

666 - (rw-rw-rw-) All users may read and write the file.

644 - (rw-r--r--) The owner may read and write a file, while all others may only read the file. A common setting for data files that everybody may read, but only the owner may change.

600 - (rw-------) The owner may read and write a file. All others have no rights. A common setting for data files that the owner wants to keep private.

* Change Ownership of a file or folder:

*chgrp new\_group some\_file*

---------------------------------------------------------------------------------------------------------------------

* Renew or release a Dynamic Ip address

*sudo dhclient*

*sudo dhclient -v -r* -manually release with -r, and -v to see what is going on

* For Ethernet and wire or any other (just replace eth0)

*sudo dhclient -r eth0*

*sudo dhclient eth0*

* Manual reboot of network

*ifdown <name of network>*

*ifup <name of network>*

*or*

*/etc/init.d/networking restart* -for Debian/ubuntu

* Setting static ip address (make sure no network manager is interfering)

/etc/network/interfaces

*auto enp0s8*

*iface enp0s8 inet static*

*address 10.0.0.41*

*netmask 255.255.255.0*

*network 10.0.0.0*

*broadcast 10.0.0.255*

*gateway 10.0.0.1*

*dns-nameservers 10.0.0.1 8.8.8.8*

*dns-domain acme.com*

*dns-search acme.com*

* DHCP enabling

*auto enp0s3*

*iface enp0s3 inet dhcp*

* On the fly but will reset after reboot

*Ifconfig <interface name> <ip address> netmask <netmask>*

*Ex. Ifconfig enp0s8 10.0.0.1 netmask 255.255.255.0*

---------------------------------------------------------------------------------------------------------------------

*#!/bin/bash*

*iptables -P INPUT DROP*

*iptables -P FORWARD DROP*

*iptables -P OUTPUT ACCEPT*

*iptables -A INPUT -i lo -j ACCEPT*

*iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT*

# allow icmp

*Iptables –A INPUT –p icmp –j ACCEPT*

# allow ssh traffic

*iptables -A INPUT -p tcp --dport ssh -j ACCEPT*

# allow http and https traffic

*iptables -A INPUT -p tcp --dport http -j ACCEPT*

*iptables -A INPUT -p tcp --dport https -j ACCEP*T