Linux Boot
Dmesg
Dmesg | grep sda/hda/nvme
Dmesg | head -20
Dmesg | grep -I usb
Journalctl -k
Journalctl -r
Journalctl -p
Lsinitrd
lsinitrd initramfs-2.6.32-22.el6.x86_64.img
dracut (add and rm modules)

Modules
Uname
Lsmod
Modinfo
Modprobe
Modprobe -r
rmmode

Network Connections
Nmcli
Nmcli device show
Nmcli connections show
Nmcli device status
Nmcli con down/up “nameOfcon”
Ncmli con delete “nameOfcon”
Nmcli con add con-name “nameofCon”
Type ethernet ifname “eth0”
nmcli con add con-name "nameofConnection" type ethernet [we need ip, gateway, and mask]
ip4 192.168.122.75/24 gw4 192.168.122.1 ifname [device]
autoconnect [bring connection up when the system starts]

nmcli con edit (prompt settings)
nmcli con mod [nameofCon] ipv4.dns “IPAddress”
nmcli -f ipv4.dns con show [nameofCon]

IP
Ip addr show
Ip route show
Ip addr add [IPaddr] dev “device”
Ip addr del [IPaddr] dev “device”
Ip -s addr
Ip link set “device” down/up
Ip route add default via [IPaddress] dev “interface”
Hostnamectl
Querying Hostnames
Host (resolve DNS)
Host localhost/google.com
Dig (query DNS servers
Getent (queries /etc/nsswitch.conf)

Partitions
Lsblk (show blocks) Legacy MBR
Fdisk -l /dev/[deviceName] Legacy MRB
Fdisk -l /dev/sda
Parted (Modern Command for MRB/GPT)
Gdisk /dev/sda (create GPT partition)

Swap Partition
Swapon –summary
ID of 82 (8200) Swap partition
Mkswap format so use as swap space
Mkswap -L SWAP /dev/[nameofnewPartition]
Swapon -L [nameoflabel]

Creating Linux FileSystem
Mkfs (creates new file system on partition)
Mkfs -t ext4
Mkfs.ext4 -L SRV /dev/sda1
Blkid

Mount Points
Mount (mount partitions to directories)
Mount -t ext4
Mount /dev/sda1 /opt (umount)
Mount -a (will scan etc/fstab
Mount /dev/sr0 /media

Maintaining a Filesystem
Fsck File system check
Fsck -r To get a report
Df -h check mount point
E2fsck for ext2/3/4 filesystem

Create filesystem
Mke2fs Creating ext2/3/4 filesystem
Mke2fs -t ext4 -L EXTRA /dev/sdb1
Tune2fs -l /dev/sda1 List parameter applied to a file
Tune2fs -I 3w /dev/sdb1 File system check every 3w

E2sck -f /dev/sda1 force to check again
E2sch -p /dev/sda1 repair errors

Disk usage space
Df -h
Du -s -h
Du -sh /tmp
Check on INODE
Ls -i
Df -i
Du –inoded

Check on INODE
Ls -i
Df -i
Du –inoded

Localization
Locale
Localectl
Localectl list-locales
Sudo localectl set-locale LANG=es_ES.utf8

Time and date
Date
Date -u
Timedatectl
Timedatectl set-time “2019-11-1 22:22:00” if no NTP server
Tzselect
Tz

Advances Packet Manager
Sudo apt-get update
Sudo apt-get upgrade
Sudo apt-get install
Sudo apt-get remove “nameofPackage”
Sudo apt autoremove to remove left dependencies
sudo apt-get purge “nameofApp” remove config files
apt-get purge rm pack of system
apt-get dist-upgrade upgrades all packs on the system
apt-get download htop to Download packages
apt-cache search srch on local apt cache
apt-cache show basic info about a package
apt-cache showpkg more tech info about a pack

Using Debian Package
Dpkg –info Displays info on a package
Dpkg –info htop_2.2.0-1.amd.deb
Dpkg –status
Dpkg -l
Dpkg -I Installs specific packages
Dpkg -L lists files installed with a specific pack
Dpkg -r rm a specific pack but leaves files behind
Pdkg -P rm a specific pack and also config files

The Yellowdog Updater Modified (YUM)
Zipper Open Suse
DNF Fedora
Sudo yum update
Yum search Searches yum repos for specific pack
Yum info lists info about a specific pack
Yum info httpd
Yum lists installed display all packs installed
Yum clean all clean cash info
Sudo yum install httpd

The Red Hat Package Manager
Rpm -qpi Displays info on a pack
Rpm -qpl lists files in a pack
Rpm -qa lists out all installed packas
Rpm -i Installas a specific pack
Sudo rpm -ivh “nameofpack”
Rpm -U upgrades and installs pack with newer ver
Rpm -e uninstalls an installed package
Sudo rpm -e “nameofpack”
Rpm -Va Verify all installed packaes

Sudo yum -y remove httpd
Sudo yum autoremove unistall a pack and its depende
Sudo yum reinstall httpd

Understanding Devices in Linux
Udev Linux device manager
/dev/dri for video cards
Lscpi displays info on PCI devs
lcpi -k check whay part of hardware is linked to mod
lsusb diplays info on USB devs
lscpu displays info on processors on a system
lsblk Displays info on all block devs

Manage Users and Groups
Useradd
Useradd -m “nameofuser” create home directory
Useradd -m -c “Daniel tapia” dtapia add comment
Passwd
Sudo passwd dtapia
Passwd -e dtapia prompt user to change password
Userdel
Userdel -r to remove user’s home directory
Rm -rf /home/dtapia
Usermod
Usermod -a -G finance dtapia
Usermod -L dtapia
Usermod -s /sbin/nologin dtapia disable bash
Chage Modify aging parameters of a user’s passwd
Chage -E 2019-01-01 dtapia
Chage -l dtapia check account information
Chage -W 14 dtapia set passwd to expire in two weeks

Adding and Removing Groups
Groupadd
Groupadd nameofGroup
Useradd -G finance -m -c “Daniel tapia” dtapia
Getent check for users and groups
Getent group finance
Getent user dtapia
Groupdel
Groupmod
Ls -l /etc/shadow check on permission on shadow file

Bash Environment
env displays environment variables
echo $variableName
export Command used to export a var to current shell
pwd
which
type
weak quotes “ “ expand variables
echo “$PATH”
strong quotes ‘ ‘ nothing is interpreted
echo ‘$PATH’

Customizing the Shell Environment
Env
Export
Set displays all Bash settings, vars and functions
Unset rm an environment var an its value
Alias is used to create a shortcut to a longer command
Alias ll=”ls -lh” not permanent change
Function Abash keyword used to indicate new bash fn
Function stuff {} {
    Ls ~
    Ls /opt
    }

Make permanent changes
Vim .bashrc

if a script is not listed in the PATH, we can create a PATH
make this change permanent?
Vim .bash_profile
PATH=$PATH:$HOME/.local/bin:$HOME/bin:$HOME/prog

"user specific aliases and functions"
Alias ll="ls -lh"
.(dot) used to source or apply functions from a file
Source .bashrc to reload changes

Automate and Schedule Jobs
* * * * *
Minute hour day month day of week
* * * * * user-name command to be executed
Crontab -e edit
Crontab -l view content
Crontab -u dtapia to view tasks

AT
Used for one-off jobs
Yum -y install at
Systemctl start atd.service
Systemctl enable atd.service
At now + 5 minutes
At> Echo "notes for later" > /root/notes.txt
at> <EOT>
at 4:00 AM tomorrow
at> rm /root/notes.txt
at> <EOT>

Create, Modify and Redirect Files
cd
mkdir
rmdir
$PATH Env var that describes dirs for current user
Ls
Touch
Cp
Rm
Rm -rf
Mv
File

File Globing
* matches zero or more
? matches any single character
[abc] matches any one of the characters in the list
[*abc] matches any one of the chars except the list
[0-9] Matches a range of numbers
Regular Expressions
. represents a single character
^ searches the beginning of a line
$ Search the end of a line
[abc] Search for specified characters
Grep g.m passwd
Grep ^rpc passwd
Sed can operate on files using regular expressions
Egrep searches a specified file line by line
Fgrep searches based on strings rather than patterns
Egrep 'bash$' passwd
Fgrep -f strings passwd

Understanding Links
Ln creates a hard link
Ln Documents/test.txt test.txt.lnk
Ln -s Creates symbolic links
Ln -s ~/bin/topprocs.sh topps.sh
Unlink removes a link from a file or folder
Unlink test.txt.lnk

Finding Files
The find command is very versatile and powerful
Find .(home directory) -name mc.sh
Sudo find / -name passwd
Find . -ctime 1 find on the time when they were last changed
Find . -atime 2 find files changed in the last 48hrs
Find . -empty find files or folders that are empty
Find . -empty -type f -exec rm -f {} \: (will delete any found files that are empty)

Standard Input, Output, and Error
Wc test.sh input from keyboard
Wc < test.sh input comes from file
Error has file handle number associated with error

Redirecting Output to the Screen and File
Echo “yep” > myfile.txt
Echo “yep some more” >> myfile.txt
Cat < myfile.txt
Cat /etc/passwd | less
Tee chaining together long commands. Copies data from standin to each FILE, and also to standout.
Ls -d /usr/share/doc/lib[Xx]* | tee lib-docs.txt
Xargs Access input from stdin and other commands
Find test/ -empty | xargs rm -f

```
find /tmp -name core -type f -print0 | xargs -0 /bin/rm -f
```

Find files named **core** in or below the directory **/tmp** and delete them, processing file names in such a way that file or directory names containing spaces or newlines are correctly handled.

Finding Command on a Linux System
Locate passwd
Updatedb updates db that locate command uses
Where is locates binary, source, and manual pages

Files and Folder Compression
Dd
Dd if=boot.img of=/dev/sdc
Dd if=/dev/xvda of=/tmp/mbr.img bs=512 count=1
Backup master boot record
Tar wraps files and folders into an archive file.
Tar -cf content-bak.tar content-lpic-1
Tar -tf content-bak.tar take a look at files without unarchive it.
Tar -xf content-bak.tar to Extract files
Gzip command that creates .gz compressed files
Tar -czf content-back.tar.gz content-lpci-1
Gunzip to extract .gz compressed files
Bzip2 Command that created .bz2 compressed files
Tar -cjf content-back.tar.bz2 contentbackup
Tar -xvjf content-bak.tar.bz2
Xz command that creates .xz compressed files

Manage Services
Runlevel check which runlevel, only one at the time.
Runlevel 0 halt
Runlevel 1 single user mode
Runlevel2 Multi-user mode
Runlevel 3 multi-user mode (with networking)
Runlevel 4 unused
Runlevel 5 multiuser, with networking and graph deskt
Runlevel 6 reboot

SystemD
Provides a aystem and service manager
Systemctl list-unit-files View all unit files.
Systemctl status httpd.service
Systemctl enable httpd.service when system boots
Systemctl is-enable <daemon> if unit to start at boot
Systemctl disable httpd.service when system boots
Systemctl start/stop httpd.service
Systemctl restart httod.service
Target Unit File
Links and group other units together
Systemctl list-unit-files -t target show all targets
Systemctl list-units -t target lists all loaded and active
Systemctl get-default list out the default target
Systemctl set-default change default target
Systemctl set-default multi-user.target
System isolate <target> Will change from current target to a different target
Systemctl isolate multi-user.target console mode
Systemctl isolate graphical.target revert change above

Review the State of Your System
Ps
Ps -eH | less
Top
Man proc
Man signal
Uptime
Free
Pgrep
Pgrep -a httpd
Pgrep -u <username>
Kill -l to see all sigterms and sigups
Pkill httpd
Killall takes process name as argument
Watch runs a command at specified intervals
Watch -n 5 date rerun command every 5 seconds
Screen terminal windows manager that allows you to run commands in an isolated session
Tmux a modern terminal windows manager with extra features

Core Network Servers

Port	Service
53	DNS TCP/UDP
123	NTP UDP
67/68	DHCP UDP
389	LDAP
363	Encrypted LDAP
88	Kerberos
514	Syslog UDP
6514	Secure syslog Comms TCP
19531	Systemd-journal TCP
161	SNMP
10161,10162	SNMP over TLS
3128	Squid Proxy TCP
3306	MySQL
5432	POstgreSQL
631	CUPS
110	POP3
995	SSL/TLS POP3
143	IMAP
993	SSL/TLS IMAP

Basic File and Folder Permission
Symbolic permissions -r -w -x
Octal permissions 4 read 2 write 1 exec 0 npermission
Modify Basic Access Mode
Chown change ownership of file/directory
Chmod change mode of a file or directory
Chgrp change the group ownership
Chmod o-r secret.txt
Chmod -R o-r Documents/*
Chmod 600 secret.txt
Chown :research reports.csv
Chrp research code_ideas.odt

Overview of SELinux
Check access denied logs? /var/log/messages
Ls -Z displays the SELinux context
Sudo semanage login -l view maping from SE users to L
Sudo semanage user -l view the SELinux users details

Modifying Advanced Permissions
SUID enables other users to run file with permissions
Chmod 4765 test.sh
Chmod u+s test.sh
SGID assigns group ownership to files. Shared groups
Chmod -R 2770 /srv/team
Umask default permissions for newly created files
777 default for directorires
666 default for files
Umask u=rwx,g=,o=
Makes changes permanent?
/etc/bashrc = umask set for the whole system
/home/<user>/.bashrc = umask set for individual user
Getfacl get file access control lists
Getfacl file 1
Setfacl -m u:jimmy:r file1

AppArmor
Apparmor_status
Sudo apt install -y apparmor-utils
Aa-confined shows nets proc that are runn on confined
Sudo aa-genprof <nameOfProfiles>

SElinux Configuration
SElinux = Enforcing, Permissive, Disabled.
Getenforce get the current configuration
Setenforce Change the current configuration
Sudo setenforce 1
Setstatus get the details of the current config
Getsebool get a list of SELinux Booleans
Semanage bolean -l get a long list of SEL booleans

Privilege Escalation
Su simply switch to another user
Su - changes session (different login shell)
Sudo
Sudoedit limits elevation to only edit text files

Whell group are allowed to run sudo commands
Visudo to edit sudoers file
Sudo visudo
If adding group to sudoers, do not forget %

PAM Basics
Plugabble Authentication Modules
Control flags:
Optional: result is ignored
Required: results is required to continue
Requisite: required with notification
Sufficient: result is ignored on failure
Password policies
Pam_pwhistory
Pam_pwquality
User lockout:
Pam_faillock
Pam_tally2
Sudo vim password-auth
Password required pam_pwhistory.so remember=30 use_authok
Auth required pam_tally2.so deny=3 unlock_time=1800 Even_deny_root

SSH Basics
Ssh <username>
Ssh cloud_user@3.17.167.1
(server will be added to list of known hosts
Ssh config on ~/.ssh
Ssh_keygen
Ssh-copy-id
Ssh-add
Ssh-keygen to use keys instead of passwords
Ld_rsa private key
Ld_rsa.pub key that is passed to remote server
Ssh-copy-id cloud_user@3.17.167.1 (remote server)
Vim ./sshd_config
  AllowUsers
  AllowGroups
Sudo systemctl restart sshd after making changes
/etc/hosts.deny
/etc/hosts.allow -> SSH and TCPWrappers
Sshd : <publicIP>,<PrivateIP>
Sudo vim hosts.deny
Sshd:ALL

Security Best Practices
Protect Boot sequence
Radius TACACS+
LDAP and Kerberos
Chrooted jail let's you simulate a directory on your fs as the root of the fs.
Cat /etc/ssh/sshd_config look for jaileduser and dir
Cryptsetup -y -v liksformat /dev/<deviceName> to encrypt device
Ls /etc/ | grep cron restrict cron access
Cron.allow Deny specific users
Securing Network Services
Disable unused insecure services
/etc/ssh/sshd_config change port
Netstat -plnt disable any unused services

Logging Services
Check var/log/directories
Logrotate roll back logging
Vim nginx manage log files
/etc/rsyslog.conf remote logging
Last show who logged in
Lastb show bad loggings
Lastlog show if user has ever logged in
Journalctl
Journalctl -f like tails
Journalctl -p err
-u for ssh
-o short output
-v verbose

Restricting Access, Remote and Local
Disable root logins
Vi /etc/passwd
Root:x:0:0:root:/root:/usr/sbin/nologin
Explicit SSH permission
Vim /etc/ssh/sshd_config
AllowUsers cloud_user

Firewall Technologies
Iptables -nL
ACL packet filter – Src/dst IP Src/dst port TCP/UDP
ACL action Accept, reject, drop

Iptables -l INPUT -p tcp -s 10.21.55.10 –dport80 -j ACEEPT
  traffic only allowed from web server inside the network.
-p packet
-s source
--d destination port

UFW uncomplicated firewall
IP forwarding routing functionality, kernel enabled
Echo 1 > /proc/sys/net/ipv4/ip_forward
Cat /sysctl.conf and uncomment the following section
Net.ipv4/ip_forward=1

Dynamic Set Rules
Uses IP sets to define rules
Allows IP sets to be updated instead of the rules
Ipset create 80_allow hash:ip
Ipset add 80_allow 192.168.1.92
Ipset list 80_allow
Trusted ports 0 – 1023 AKA privileged ports

Directories

/boot/grub

Grub.conf/menu.lst (RHEL)

Device.map (Debian)

/etc/default/grub (Main Config file)

/etc/groub.d (Config Files)

/etc/dracut.conf.d (Add-RM modules)

/lib/modules

/etc/modprobe.d (Prevent modules from loading)

/etc/modprobe.d/floppy-blacklist.conf (Edit)

Blacklist floppy

/proc/sys/kernel/panic (Not permanent if changed)

/etc/sysctlconf kernel.panic=15

/etc/hosts (localhost)

/etc/hostname (computer's hostname)

/etc/resolv.conf (IP addrs of DNS servers)

/etc/nsswitch.conf (Determine order of DNS)

Linux Environment

/proc (processes running)

/proc/cpuinfo

/sys (System's hardware and kernel modules)

/sys/fs File system

/proc/swaps (Swap usage)

/etc/fstab (to make permanent changes SWAP)

/etc/mtab (Mount command info)

Media (CR ROM)

Mount /dev/ser0/media

Software Installation

/etc/apt/sources.list APT reads from here

/etc/yum.conf Global config

/etc/yum.repos.d reads repository info

/var/cache/yum Caches latests repo info

/var/lib/rpm thr rpm database

Shared library locations

/lib

/usr/lib

/usr/local/lib

/usr/share

/etc/ld/so.conf install an app that comes with its own library file.

Devices In linux

/dev Contains information on all of the connected hardware on a system

User and groups

/etc/passwd db that contains info on user and system account

/etc/shadow This file contains encrypted password for accounts

/etc/group group definitions along with what members belong to each

/etc/skel contains items that will automatically get added to a new user when home dir is created

/etc/default/useradd config file is referenced by the useradd command

/etc/nologin can be used to display a message on the console when someone attempts to login with an account that is using the /sbin/nologin shell

Bash config

/etc/profile first file read on a login session. Sets up system-wide environment var

/etc/profile.d dir that contains extra script config on files for Bash

/etc/bashrc you can config system-wide functions and aliases here

/etc/skel dir that contains the default .bash_profile, nashrc, and others

Crontab

/etc/cron.hourly

/etc/cron.daily

/etc/cron.weekly

/etc/cron.monthly

/etc/cron.d Directory that contains cron jobs

/etc/cron/deny users listed in this file are prevented from scheduling tasks

SystemD

/usr/lib/system/system

/etc/systemd/system

/run/systemd/system

Sudo Configuration

/etc/sudoers (use visudo to edit this file)

Authentication

/etc/pam.d

Password-auth

System-auth

SSH

~/.ssh directory hidden

Known_hosts

/etc/ssh agent configuration

Ssh_config client configuration

Sshd_config SSH daemon

Vim /etc/ssh/sshd_config change default port

Logging Services

/var/log/syslog/

/var/log/messages General system traffic

/var/log/auth.log authentication attempts against the machine

/var/log/secure Authentication messages used in RHEL

/var/log/<applicationName>

/etc/logrotate.d

Journalctl

/etc/systemd/journal.conf File disappears after shutting the machine down

Var/log/journal create this directory to make the journal permanent

Commo Application firewall configuration

/etc/services