

Linux+ XK0-004

Notes By:

=====

Siddhant G. (geekat7)

<https://www.youtube.com/geekat7>

<https://www.instagram.com/geekat07/>

=====

Servers

Daemon Process:

- often ends w letter 'd'
- original super saver program was 'inetd (internal daemon)'
- configuration file : /etc/inetd
- xinetd : extended version, ACL, logging features, schedules.
- /etc/services : contains all the ports defined by a server.

L : Linux

A : Apache

M : MySQL

P : PHP

=====

Serving Local Network:

NFS : nfs-utils

Samba : Microsoft

Print Servers : CUPS (Common Unix Printing System)

IP Addresses (DHCP):

1. dhclient
2. dhcpd
3. pump

☐ **Most debian and red hat will install dhclient.**

Logging:

/var/log directory

1. rsyslogd : sysvinit & upstart
2. journald : systemd

Name Server:

BIND program : named

SNMP : net-snmp package

NTP : ntpd

=====

Security:

Password : /etc/passwd & /etc/shadow

NIS (Network Information Directory) : nis-utils is an open source package.

Kerberos : SSO

LDAP

CA (Certificate Authority):

To log into server, clients should have 2 things - Certificate file + PIN

OpenSSL

**ALREADY KNOW: <VPN, Proxy Server, Monitoring, Cluster, Container,
Load Balancing >**

Files, Directories & Text

ls : list

pwd : present working directory

ls -a all file incl. hidden

ls -d directory

ls -F file's type

ls -i all file and subdirectory

ls -l file type, permission, hard link counter, owner, group, date,
file name

ls -R shows whole tree

ls -lh makes file size more human readable

=====

touch : make a file on fly

mkdir : make directories

cp : copy

mv : move

cp -a archive
files' original attributes

recursive copy, keep all the

cp mv -f force
destination file

overwrite any preexisting

cp mv -i interactive

ask before overwriting

cp mv -n no-clobber

do not overwrite

cp -r/R recursive

copy a directory's contents

cp mv -u update

overwrite preexisting files

cp mv -v verbose

=====

rsync : lightning-fast copies of big files, backups, copy files over network

rsync -a archive : -rlptgoD

rsync -D retain device and special files

rsync -g retain file's group

rsync -h display any numeric output in a human readable format

<i>rsync -l</i>	<i>copy symbolic links</i>
<i>rsync -o</i>	<i>retain owner</i>
<i>rsync -p</i>	<i>retain permissions</i>
<i>rsync -r</i>	<i>recursive</i>
<i>rsync -t</i>	<i>retain file modification time</i>
<i>rsync -v</i>	<i>verbose</i>

=====

rm : removing files

rmdir : remove directories

<i>rm -d</i>	<i>delete any empty directories</i>
<i>rm -f</i>	<i>force</i>
<i>rm -i</i>	<i>interactive (ask before delete)</i>
<i>rm -r/R</i>	<i>recursive</i>
<i>rm -v</i>	<i>verbose</i>

=====

Linking Files & Directories (Command : ln)

Hard Link :

- *hard link allows us to create a pseudo-copy of a file.*
- *typically used in file backups.*
- *original file and hard link share same data and same **inode** number.*
- *can exists in different directories but must be on same file system.*

```
root@kali:~/Desktop# ls -lhi
total 8.0K
921895 drwxr-xr-x 2 root root 4.0K May 30 22:25 Linux+
658215 -rw-r--r-- 1 root root 13 May 30 22:24 test
root@kali:~/Desktop# cat test
first
second
root@kali:~/Desktop# ln test test1
root@kali:~/Desktop# ls -lhi
total 12K
921895 drwxr-xr-x 2 root root 4.0K May 30 22:26 Linux+
658215 -rw-r--r-- 2 root root 13 May 30 22:24 test
658215 -rw-r--r-- 2 root root 13 May 30 22:24 test1
root@kali:~/Desktop# cat test1
first
second
```

Soft Link:

- soft link provides a pointer to a file.
- do not share same **inode** number.
- file or soft links can exist in different directories or even different file systems.
- can be a security risk if a stale or dead link is there.
- readlink -f softtest

```

root@kali:~/Desktop# ls -lih
total 8.0K
921895 drwxr-xr-x 2 root root 4.0K May 30 22:32 Linux+
658215 -rw-r--r-- 1 root root 6 May 30 22:35 test
root@kali:~/Desktop# ln -s test softtest
root@kali:~/Desktop# ls -lih
total 8.0K
921895 drwxr-xr-x 2 root root 4.0K May 30 22:32 Linux+
658216 lrwxrwxrwx 1 root root 4 May 30 22:35 softtest -> test
658215 -rw-r--r-- 1 root root 6 May 30 22:35 test
root@kali:~/Desktop# cat test
first
root@kali:~/Desktop# cat softtest
first

```

=====

Reading Files :

cat : reading text file

cat -n	line column
cat -m	(merge) used while displaying multiple file
cat -t	(omit header)

grep : searching for a particular string

grep -i	ignore case-sensitive
grep -d skip	

head, tail

head -n <number>

more, less

Less is More

More : Space key to next page and Enter to next line.

Less : Faster cause it doesn't read the entire file prior to displaying file's first page. Scroll, Up-Down keys.

Diff : explore the differences between text files

diff -e used to make the first file compared the same as the second file

diff -q brief message (Files abc.txt and def.txt differ)

diff -s if same, simple message

diff -y side by side comparison

diff -r recursive

which : locate the commands

whereis : locate binaries of the program

locate : finding files

locate -A display file and directories names matches all the patterns

locate -b display only those file names that matches the pattern

locate -c count

locate -i ignore-case

locate -q do not display error

locate -r use regex

locate -w default behavior (whole name)

find : complex, able to find file using metadata

find -cmin <n> display names of files whose status changes
n minutes ago

find -mmin display names of files whose data changes n
minutes ago

find -empty

find -gid, -gname group ID and/or name

find -inum inode

find -maxdepth directory's level

find -nogroup

find -perm whose permission matches either octal/-
symbolic modes

find -size

find -user <name> *display files whose owners are name*

=====

Search and Analyze Text

cut

cut -c <1-2> : Character

cut -b <2-3> : Bytes

cut -d "<character>" -f 2 : Delimiter

grep

grep -c : count

grep -i : ignore case

grep -r : recursive

grep -d <action> : directories

grep -v : invert match

sort

printf

wc

wc -c : byte count

wc -L : byte count of the file's longest line

wc -l : file's line count

wc -m : file's character count

wc -w : file's word count

=====

Redirecting IO :

Linux treats every object as file.

STDOUT : directs output to current terminal

STDERR : directs errors

Process's current terminal is represented by /dev/tty file.

Redirection Operators

> overwrite

>> append

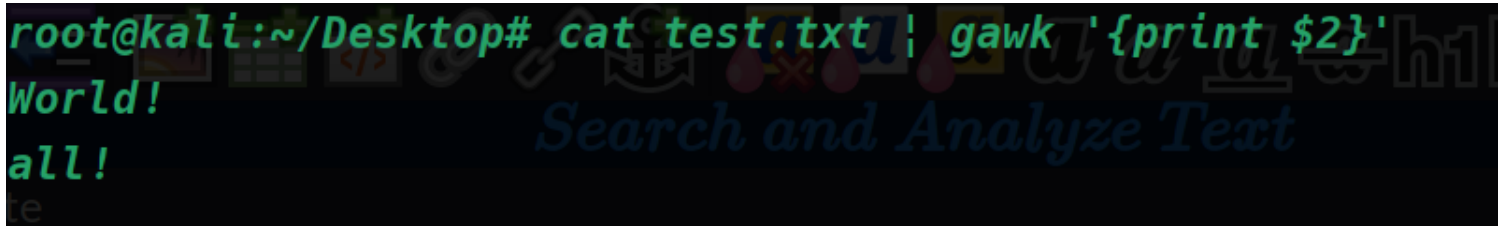
2> redirect STDERR, overwrite
 2>> append
 &> redirect STDOUT and STDERR, overwrite
 &>> append
 < STDIN to command
 <> STDIN from specified file to command and redirect STDOUT to file

=====

Stream Editors :

cat abc.txt | sed 's/one/twenty/'
 sed -e 's/one/twenty/ ; s/two/fourty/' abc.txt
 sed -f script.sed abc.txt (use a script)

gawk



```

root@kali:~/Desktop# cat test.txt | gawk '{print $2}'
World!
all!
  
```

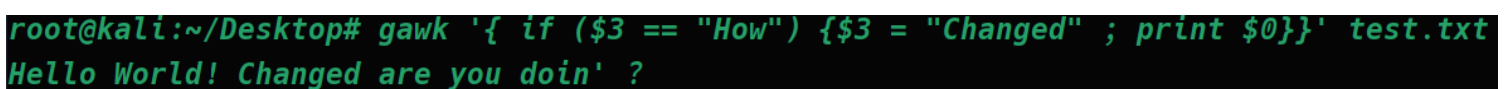
\$0 : Entire text line
 \$1 : first data field
 \$2 : second data field

||

....

||

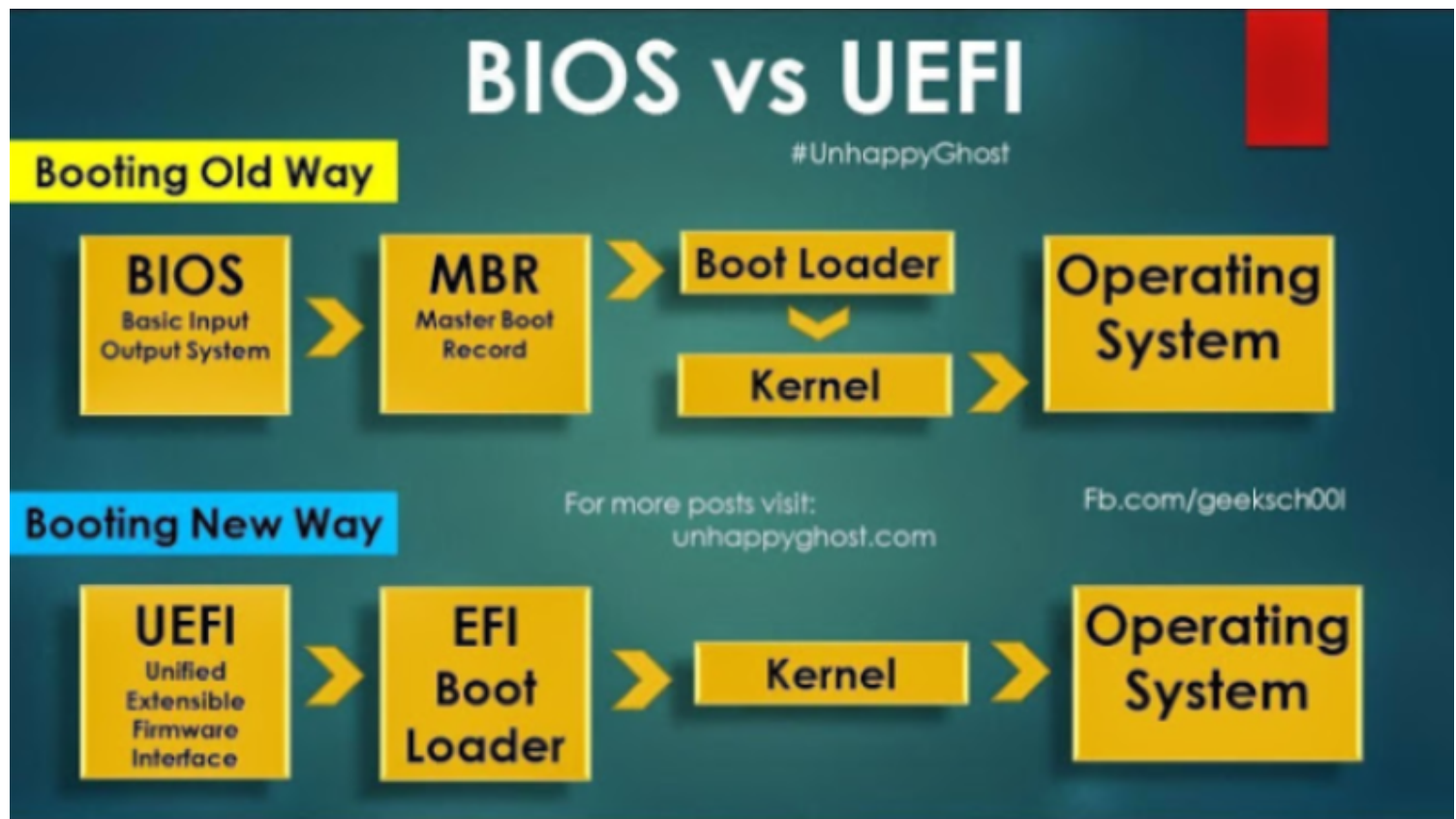
gawk '{print \$1}' test.txt
 gawk '{\$3="Hi!"; print\$0}' test.txt



```

root@kali:~/Desktop# gawk '{ if ($3 == "How") {$3 = "Changed" ; print $0}}' test.txt
Hello World! Changed are you doin' ?
  
```

Boot Process



□ **BASICS :**

POST (Power on Self Test) : BIOS/UEFI : Looks for Boot Loader program.

||

∨

BOOTLOADER (LILO/GRUB/GRUB2) : Determines what Linux kernel program to load.

||

∨

Kernel loads into memory & starts the necessary bg. checks.

=====

- > **Kernel Ring Buffer** : Boot messages are copied into kernel ring buffer.
- > **dmesg** : command to view the boot msg. and troubleshoot.
- > **Boot logs** : /var/log/boot.log

```

[ 0.000000] Linux version 5.10.0-kali8-amd64 (devel@kali.org) (gcc-10 (Debian
10.2.1-6) 10.2.1 20210110, GNU ld (GNU Binutils for Debian) 2.35.2) #1 SMP Debi
an 5.10.40-1kali1 (2021-05-31)
[ 0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.10.0-kali8-amd64 root=UU
ID=6f40f0f1-54b1-4dfb-a3fc-00b9a392a346 ro quiet splash
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point regi
sters'
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[ 0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[ 0.000000] x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
[ 0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes,
using='compacted' format.
[ 0.000000] BIOS-provided physical RAM map:
[ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009ebff] usable
[ 0.000000] BIOS-e820: [mem 0x000000000009ec00-0x000000000009ffff] reserved

```

=====>

❑ FIRMWARE

1. **BIOS** (Basic Input/Output System):

- > simplistic menu setup
- > could read only 1 sector data from HDD, not enough space to load an entire OS
- > BIOS must know where to find OS.
- > Most BIOS allows to load bootloader from multiple locations i.e. HDD, CD, ISO, USB, Network Server, etc.
- > While booting from HDD, we define MBR to designate HDD.

2. **UEFI** (Unified Extensible Firmware Interface):

- > New (2005)
- > Instead of relying on a single boot sector like MBR, UEFI specified special disk partition called ESP (EFI System Partition).
- > it is mounted on /boot/efi and bootloader files are stored with 'efi' extension.

Firmware's job is just to find and run the bootloader.

□ **BOOTLOADER**

1. **LILO** (Linux Loader):

- > OG bootloader
- > doesn't work with UEFI
- > In older linux, it can be found @ /etc/lilo.conf

2. **GRUB Legacy** (Grand Unified Bootloader):

- > 1999, replaced LILO
- > simplified the process of creating boot menus and passing out to kernels.
- > interactive shell to customize boot process on the fly.
- > GRUB Legacy stores the menu commands in menu.lst OR grub.conf (Redhat) under /boot/grub.
- > initrd command defines boot time RAM disk.
- \$ grub-install /dev/sda
- \$ grub-install '(hd0)'

3. **GRUB2** :

- > 2005, new version
- > GRUB Legacy stores the menu commands in grub.cfg OR grub2.conf (Redhat) under /boot/grub.
- \$ grub-mkconfig > /boot/grub/grub.cfg [Update the configuration file from GRUB to GRUB2].

There are some alternative Bootloaders :

SYSLINUX (FAT), EXTLINUX (Mini bootloader ext2, ext3, ext4, or btrfs), ISOLINUX (LiveCD), PXELINUX (Network Server), MEMDISK (boot DOS), etc.

Bootloader's job is just to point to the kernel of the OS.

=====>

□ **SYSTEM RECOVERY**

1. **Kernel Failure** : when the linux kernel stops running in memory, causing linux system to crash ["Kernel Panic"]. Often, it can be fixed by editing the necessary files to change the system.

- > Selecting Previous Kernels at boot
- > Single-User Mode : adding 'single' command into GRUB, system will boot into runlevel 1.
- > Passing Kernel Parameters : you can add other kernel parameters to linux command in boot menu (drivers, etc).

2. **Root Drive Failure** : Bootloader can't read the root device.

- > Using a Rescue disk : **fsck /dev/sda1**
fsck will examine the inode table along with the file blocks and an attempt to reconcile them. If error occurs, you'll be prompted with an screen, add -y to auto answer 'yes' to them.
- > After completing fsck process, you can test the repaired partition by mounting it to the virtual directory. examine and the unmount. Reboot the system using standard settings.

Systemd

init (Initialization Daemon) :

- Determines which services and in what order they will be started.
- Can be located at /etc/, /bin/ or /sbin/
- Typically has a PID of 1

```
root@kali:~# ps aux | grep init
root      1  0.6  0.2 164236 10392 ?        Ss   20:35   0:02 /sbin/init splash
```

- The program is usually linked to systemd

```
root@kali:~# readlink -f /usr/sbin/init
/usr/lib/systemd/systemd
```

SYSTEMD :

- Introduced a new shift in how Linux manages the services.
 - ☐ Services can now be started as :
 - ☐ when system boots
 - ☐ when any hardware attaches
 - ☐ when certain other services are started
 - ☐ also can be based upon timer

SYSTEMD UNIT Files :

- Unit defines a service, a group of service or an action.
- Unit contains Name, Type, Configuration File. Currently there are 12 unit types :

\$ systemctl list-utils

automount	device	mount	path	scope	service	slice	snapshot	socket
-----------	--------	-------	------	-------	---------	-------	----------	--------

- Group of services are launched via 'target' unit files. default.target unit is

responsible for it.

```
$ systemctl get-default
```

```
$ readlink -f /etc/systemd/system/default.target
```

- The master systemd is in `/etc/systemd/system.conf`

Service Unit File :

- Service unit contains info as which environment file to use, when a service must be started, what targets want this service started, etc.
- In case of 2 duplicate service configuration files, priorities (ascending) :
 - `/etc/systemd/system`
 - `/run/systemd/system`
 - `/usr/lib/systemd/system`

`$ systemctl list-unit-files` > lists out the states of unit files.

enable- d = starts at system boot	disable- d = doesn't start at boot	static = starts if another unit depend- s on it or manua- lly
--	---	--

- For service unit files, there are three primary configuration sections:
`[Unit]` `[Service]` `[Install]`

```
root@kali:/usr/lib/systemd/system# cat apt-daily.service
[Unit]
Description=Daily apt download activities
Documentation=man:apt(8)
ConditionACPower=true
After=network.target network-online.target systemd-networkd.service NetworkManager.service
connman.service

[Service]
Type=oneshot
ExecStartPre=-/usr/lib/apt/apt-helper wait-online
ExecStart=/usr/lib/apt/apt.systemd.daily update
```

[Unit]

After	Sets this unit to start the designated units.
Before	after
Description	Describes the unit.
Documentation	Sets a list of URIs that points to documentation sources.
Conflicts	Sets this unit to not start with designated unit.
Requires	start together with
Wants	designated unit. if designated do not start, this won't start.
	this will still start.

[Service]

ExecReload	Script or commands to run when unit is reloaded.
ExecStart	started.
ExecStop	stopped.
Environment	sets environment variable.
Environment File	indicates file that contains env variable substitutes.
RemainAfterExit	yes/no > if yes, service is left active even when the process started by ExecStart terminates.
Restart	restarted when the process started by ExecStart terminates. Ignored if a systemctl restart/stop command is issued.
Type	sets the startup type.

• Linux uses Environment variable to store information about the shell session and working environment.

```
$ systemctl --no-pager cat apache2.services
```

[Install]

Alias	sets additional names that can be used to
denote service	
Also	additional unit
RequiredBy	designates other units that require this service
WantedBy	designate which target unit manages this service

Target Unit File :

Purpose of target unit file is to group together various services to start at system boot time

default.target is linked to the target unit file used at system boot

\$ systemctl get-default

=====

Modify System Configuration Files :

*Do not modify files in /run/systemd/system/ OR /usr/lib/systemd/system/
Copy files to /etc/systemd/system/ and then modified files will take precedence over others*

systemd-delta : check if any other unit files override this or not

systemctl daemon-reload : changes to take effect (Load unit configuration file)

systemctl reload : load service configuration file

get-default : system's default target (usually its graphical.target)

set-default : change

isolate : jump between the system targets

\$ systemctl isolate multi-user.target

Rescue target : system mounts all the local system, only root is allowed

Emergency target : system only mounts root file system

\$ systemd-analyze

SysVinit

Runlevels

\$ runlevels

0	Shut down
1	Single user mode used for system maintenance
2	Multi-user mode without networking services enabled (Security Issues)
3	Multi-user mode with networking services enabled
4	Custom
5	Multi-user mode with GUI
6	Restart

How to know you are running [SysVinit](#)

\$ ps aux -> process no 1

\$ ls -l /sbin/init

In case of sysvinit, series of scripts run at boottime, Kernel executes /sbin/-init

sysvinit runs /etc/rc.d/rc.sysinit script

Each runlevel maintains its own set of scripts : /etc/rc.d/rc#.d

> see current runlevel : \$ who -r

> run \$ init # or telinit #, add "-t 60" for 60 seconds delay.

Set services to Boot

\$ chkconfig service_name on/off : enable/disable services at current runlevel

\$ chkconfig --level 2 service_name on/off

\$ chkconfig --list

Networking

☐ **Network Configuration files :**

/etc/network/interfaces : Debian

/etc/sysconfig/network-script : RedHat

Network Manager is the GUI based tool to configure network :

☐ **NMCLI :**

\$ nmcli device status

\$ nmcli device show eth0

\$ nmcli connection show eth0

\$ nmcli connection reload eth0

\$ nmcli connection down eth0

\$ nmcli connection up eth0

\$ nmcli connection edit eth0

☐ **Legacy :**

\$ ifconfig

\$ ethtool

\$ iwconfig

'ip' utility replaces it all : \$ ip addr, \$ ip addrlabel, \$ ip route, \$ ip neighbor, \$ ip tcpmetrics

\$ route add default gw 1.1.1.1

☐ **DHCP :**

\$ dhclient -r

\$ 'dhcpcd' is also used in some distros

☐ **Global Options :**

/etc/sysconfig/network : applies to all network interfaces
/etc/resolv.conf : DNS
/etc/hosts : overrides DNS
/etc/hostname : defines machine's hostname

☐ **Troubleshooting :**

DNS :

\$ dig
\$ nslookup
\$ host

Transport Layer :

\$ netstat
-t : TCP
-u : UDP
-l : list of application
-s : show different types of packets used on the nw

\$ ss -antp (Examine Sockets/Port)

Restart Network Stack :

\$ service network restart
\$ systemctl restart network.service

GUI

☐ **GNOME :**

Created around late 90s

CentOS, Ubuntu uses it.

GNOME2 came and it was more traditional desktop user interface.

The most interesting feature is the Panel that contains system tray.

☐ **KDE (Kool Desktop Environment) Plasma :**

*Known to be a good desktop environment for people new to Linux
various customization options*

☐ **Cinnamon :**

*Start in 2011 when GNOME3 was not well received by many users.
created as a fork of GNOME3.*

Managed by Mint Dev team.

Fedora.

☐ **MATE :**

Started in 2011 after GNOME3.

Created by Arch-Linux distribution team.

☐ **Unity :**

Started by Canonical in 2010.

It was default on Ubuntu. In 2017, it stopped.

Provided UI experience for workstation, tablets, and Mobile devices.

=====

☐ **GUI Architecture :**

Desktop < ----- > Windows Manger < ----- > Display Server

Each desktop environment has its own default window manager : Mutter, Kwin, Muffin, Marco, and Metacity.

Display server is a program that manages communication between UI and OS.

Display server has 'Compositor' that arranges various display elements within a window to create screen images which passed back to the users.

☐ **X11 :**

The X windows system (X for short).

Until 2004, the dominant server implementing X was XFree86.

X11 has some security vulnerabilities. Hence, getting replaced by wayland.

configuration stored at /etc/X11/xorg.conf OR /etc/directory

Typically this file no longer is used. It created a session config on the fly.

```
$ Xorg --configure
```

```
$ xwininfo
```

```
$ xdpinfo
```

☐ **Wayland :**

Released in 2009, Replacing X11

Simpler, more secure, easier to develop and maintain.

To enable/disable wayland : /etc/gdm3/custom.conf

=====

☐ **Using Remote Desktop :**

VNC :

Virtual Network Computing is multi-platform and uses a remote frame buffer.

Offers GUI services at port 5900 + n (n = number of displays).

VNC can be used with Java enabled web browser on 5800 + n

Does not provide any traffic encryption by default.

Xrdp :

Support RDP

Uses X11rdp or Xvnc to manage GUI sessions

Comes systemd ready
TLS 1.0 encryption, simple to use

NX :

Created by nomachine around 2001
Excellent response time, faster than VNC
OpenSSH tunneling support by default
Supports multiple simultaneous users through a single network port.

SPICE (Simple protocol for independent computing environments) :

Supports multiple data socket connection, so you can have multiple clients.

Allows high quality video stream.

Provides live migration features.

Strong security features with TLS and SASL.

☐ **Forwarding :**

One way to provide security for remote client/server architecture is SSH port forwarding.

It allows you to redirect connection from a particular network port to 22.
Similar to VPNs.

You must have OpenSSL installed and enabled.

`$ systemctl is-active sshd`

In OpenSSH config file `/etc/ssh/sshd_config` : you need to allow TCP forwarding.

SSH Forwarding comes in 3 flavors : Local, Remote, Dynamic.

Local :

OpenSSH client on your system -----> Client's OpenSSH server <-----

SECURE-----> Destination Server

`ssh -L local-port:127.0.0.1:remote-port -Nf user@destination-host`

This command just establishes tunnel not remote desktop.

Remote :

Starts on the destination host

`ssh -R local-port:127.0.0.1:remote-port -Nf user@client-host`

One additional option is to tunnel your X11 connection, to check this option :

\$ grep "X11Forwarding" /etc/ssh/sshd_config

Localization

☐ Character Sets

ASCII : uses 7 bits to store english characters

Unicode : international standard uses 3 byte code to represent every language on the planet

UTF : transform long unicode to either 1 byte (UTF-8) or 2 byte (UTF-16)

`$ locale`

`language_country.character set`

☐ Setting your Locale

Manually :

`$ export LC_MONETARY=en_GB.UTF-8` : Individual LC

`$ export LANG=en_GB.UTF-8` : All the LC environment variables

`$ localectl`

`$ localectl set-locale LANG=en_GB.utf8`

☐ Time

`$ date`

Link the appropriate `timezonefile` template file from `/usr/share/zoneinfo` to `/etc/timezone` or `/etc/localtime`

Legacy Time commands :

`$ date + "%A, %B, %d, %Y"`

%A: Full weekday name, %B: Full month name, %d: Numeric day of the month, %Y: Full year

`$ timedatectl`

This command shows every system time including NTP & RTC : hardware clock

`$ hwclock`

\$ time

Displays amount of time it takes fro a program to run on the Linux system.

real: elapsed amount of time between start and end of the program

user: amount of user CPU time the program took

sys: amount of system CPU time the program took

User & Groups

☐ **Super User :**

`su <username>`

`visudo`

`user/group machine=commands`

`insid ALL=ALL`

`useradd insid -c "Siddhant G" -s /bin/bash -d /home/insid`

`userdel`

`usermod`

`chsh -s /bin/nologin insid`

`chage -l insid`

☐ **Default values :**

`useradd -D`

`/etc/login.defs`

`/etc/default/useradd`

`/etc/skel`

=====

☐ **Group commands :**

`groupadd <groupname>`

`groupmod -n <new_name> <old_name>`

`gpasswd -a <user> <group> add`

`-d : remove`

`-A : admin`

`getent passwd/shadow <user>`

`getent group <group>`

`groups <user>`

Storage

☐ **Types :**

MBR : 4 partition

GPT : 128 partition

fdisk -l /dev/sdb1 (MBR)

gdisk /dev/sdb2 (GPT)

parted /dev/sdb3

☐ **Filesystems:**

EXT [2,3,4] : Debian

XFS : RHEL 7

BTRFS : non RHEL, currently in test

*ls -la /usr/sbin/mk**

mkfs -t ext4 /dev/sdb1

mkfs.ext4 /dev/sdb2

mkswap /dev/sdb3

Label:

e2label /dev/sdb1 Primary

xfs_admin -L Secondary /dev/sdb1

mount/umount

permanent change can be made at /etc/fstab

=====

☐ **Linux File Structure :**

/bin/ - Essential user command binaries, Available to all users

/sbin/ - System binaries, Required for the system to boot

/usr/bin/ - Most user commands

/usr/sbin/ - Non-essential standard system binaries
/opt/ - Contains software not included with the installation
/boot/ - Contains boot files and the Linux kernel
/dev/ - Contains device nodes representing hardware
/etc/ - Contains configuration files
/mnt/ - Contains temporary mount points for media
/proc/ - Virtual file system containing data files for processes on the system
*/sys/ - Virtual file system containing data for hot plug devices. Similar to /
proc/*
/usr/ - Contains binaries and data sharable between users
Mounted read-only per FHS
/var/ - Contains variable data for programs in /usr/

Adv File Permissions

☐ **FACL (Filesystem ACL):**

Must be enabled at /etc/fstab

\$ setfacl -s u:<uname>:rwx filename

s : sets

m : modifies

x : removes

\$ setfacl -m g:<gname>:rw filename

Directories:

\$ setfacl -s d:u::rw directory

☐ **Sticky Bit :**

chmod o+t directory

Allows for friendly shared directories.

Backup & Restore

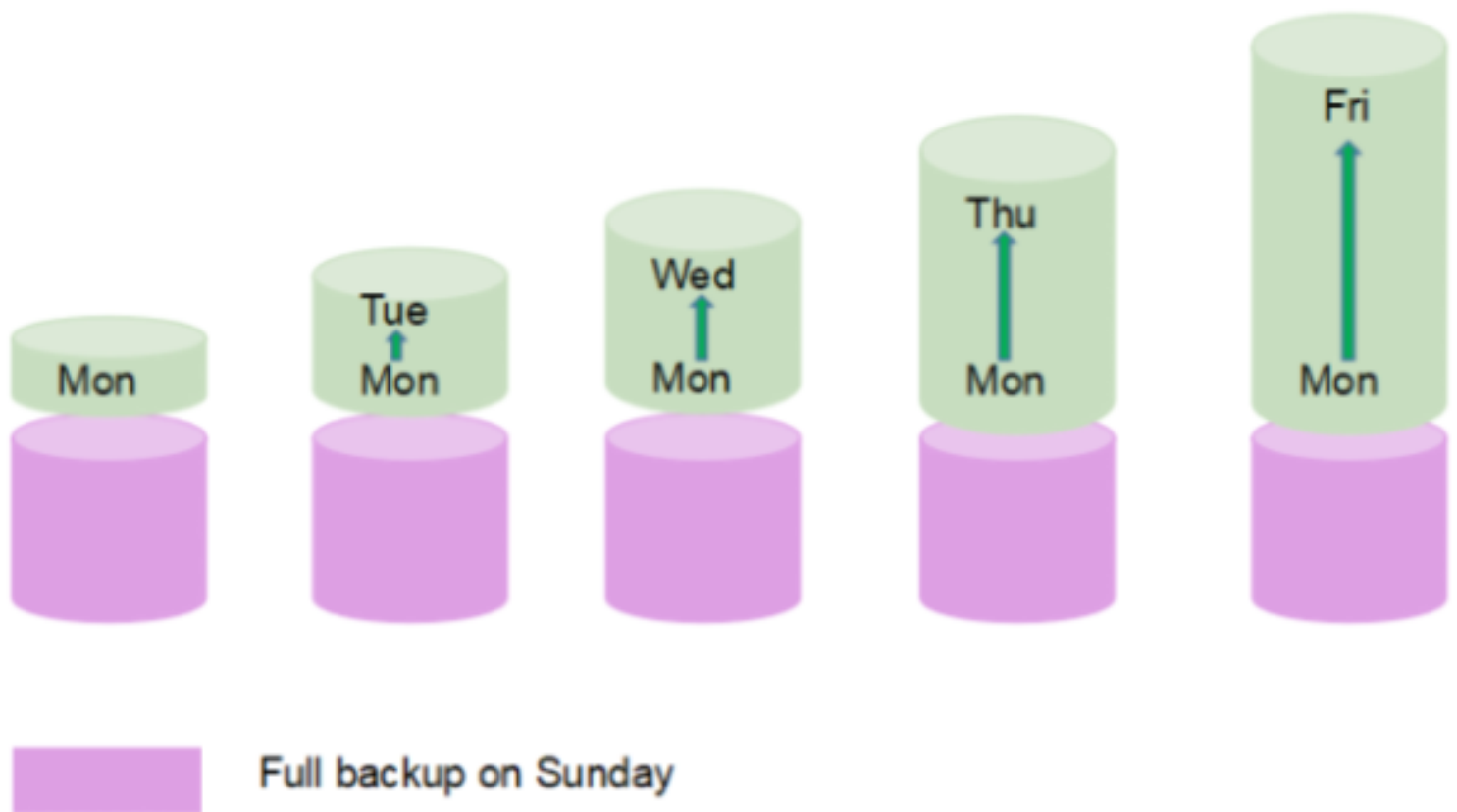
☐ Backup Types :

Full

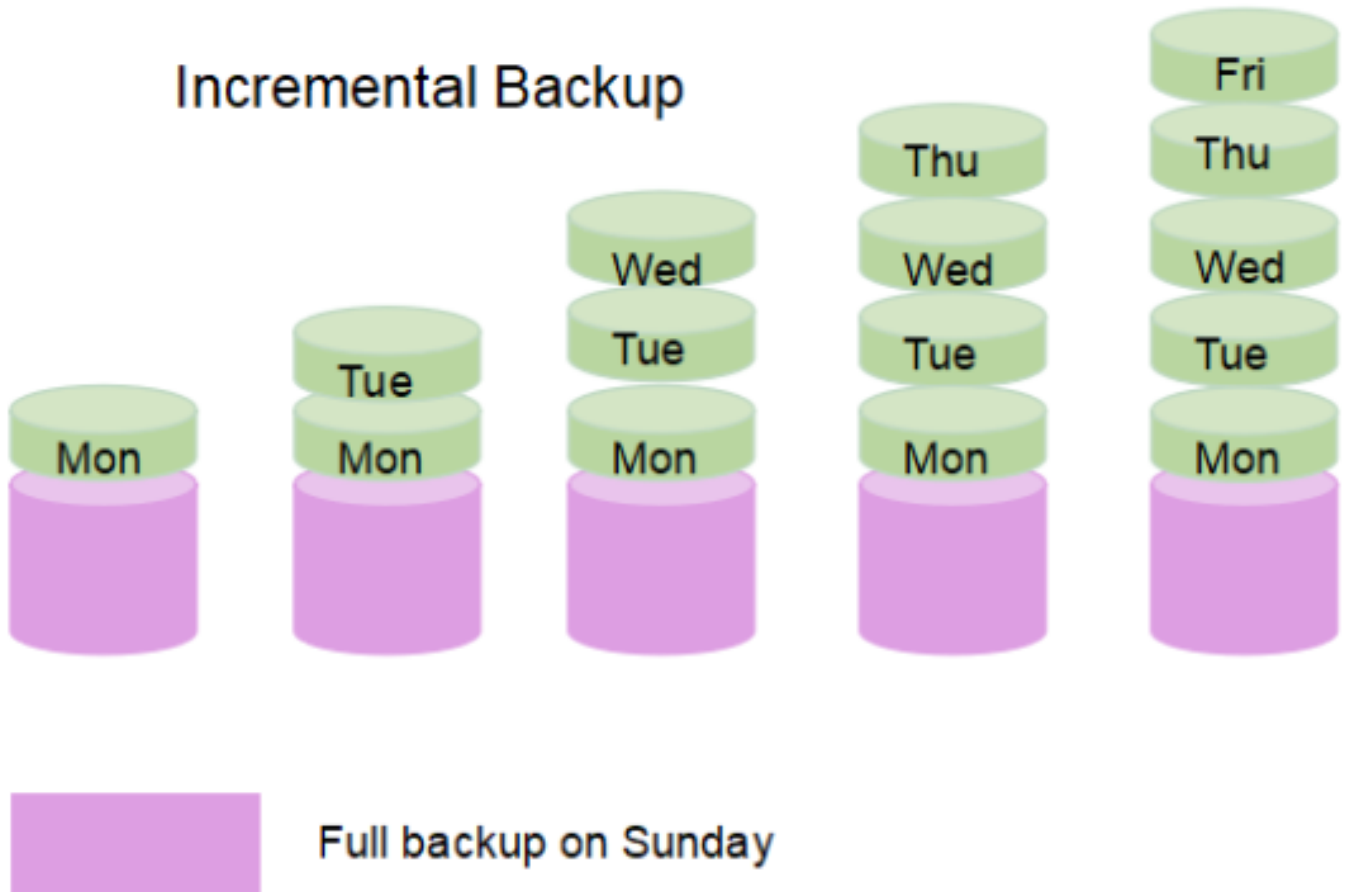
Differential

Incremental

Differential Backup



Incremental Backup



=====

☐ **Utilities to backup :**

☐ **tar :**

```
$ tar cvzf backup.tgz ~/Documents
```

c : compress/create

v : verbose

z : zip

f : filename

```
$ tar xvzf backup.tgz
```

x : extract

In tar, there is no support for differential & incremental backups. We need to use dar for the same.

tar = tape archive dar = disk archive

☐ **dar :**

Full :

```
$ dar -R ~/home/imsid -c fullbackup.bak
```

Differential :

```
$ dar -R ~/home/imsid -c fullbackup.bak
```

```
$ dar -R ~/home/imsid -c differential1.bak -A fullbackup.bak
```

Incremental :

```
$ dar -R ~/home/imsid -c fullbackup.bak
```

```
$ dar -R ~/home/imsid -c incremental1.bak -A fullbackup.bak
```

```
$ dar -R ~/home/imsid -c incremental2.bak -A incremental1.bak
```

```
$ dar -x full.bak
```

```
$ dar -x incremental1.bak -w
```

☐ **dd (Copy and Convert) :**

Can clone an entire disk

Copy a disk to another disk

```
$ dd if=/dev/sda of=/dev/sdb (Copy a disk to another disk)
```

```
$ dd if=/dev/sda of=drive_image.img (Make an image of a disk)
```

```
$ dd if=drive_image.img of=/dev/sdb (Restore)
```

=====

☐ **Other Utilities :**

mirrorvg : The mirrorvg command takes all the logical volumes on a given volume group and mirrors those logical volumes.

scp : quickly transferring file a files in a non interactive manner between two systems on a network. Uses OpenSSH. Best used for small files.

```
$ scp filename.txt user@192.168.1.1:~
```

C : compress

p : preserves file access

sftp : transfer files securely across network

\$sftp user@192.168.1.1

bye, exit, get, reget, ls, lls, mkdir, lmdir, progress

rsync : local or remote and its best to create backup

Managing Software and Kernel

apt-get (OLD)
apt (NEW)

/etc/apt/sources.list

\$ apt list <name>
\$ apt search <name>

\$ apt update/upgrade/dist-upgrade/remove

yum install/list/search/info/remove

*/etc/yum.repos.d/**
/etc/dnf/dnf.conf

dnf is the new one, eventually yum is gonna move to dnf.

=====

☐ **Building from Source :**

GCC, Make and Kernel Source are the prerequisites.

\$ wget www.software.com/sft.tar.gz
\$ tar -xvzf sft.tar.gz
\$ cd sft.tar.gz /src (Move software to src folder)
\$ make config
\$ make
\$ make clean linux-x86-64
\$ clean
\$ oldconfig
\$ sudo make install

=====

☐ **Kernel Modules :**

uname -a : see information about kernel

Load kernel :

**.ko files*

/lib/modules

/usr/lib/modules

lsmod : list modules

modinfo

insmod : install

rmmod : remove

modprobe : activate installed modules

sysctl -a