1. Introduction to linux for Cyber security

- Why Hacker use linux ?

1. Open source (Full control)
   - Linux is open source → anyone can see the code.
   - Hackers can modify tools, automate tasks, create scripts.
   - No hidden backdoors like in some proprietary OS.
2. Powerful Command line
3. Better Networking and security tools.
4. Customization.
   - Hackers can build their own OS, modify the kernel, write custom exploits.
5. Stability and performance.

2. Kali Linux vs Parrot OS vs Ubuntu - Differences.

Feature	Kali linux	Parrot OS	Ubuntu
Purpose	Professional pentration testing	Pentesting + Privacy + Lightweigh	General-Purpose O
Tools	- 600+ Security tools (Preinstalled)	+700+ tools (Pentest + Forensic)	Tools must be manually installed.
Security level	High	Very High	Medium
Performance	Heavy	Light Weigh d Faster	Very Stable
Use cases	Red teaming exploit development	Pentesting + anonymity	Learning linux development.

- Basic System Structure

Linux uses a tree-like structure where everything starts from root directory /.

Whindow has multiple drive (C:, D:), but linux has only one root.

1. Root Directory /

- The top most directory in Linux.
- Every file and folder is inside /.

```
/
├ home
├ etc
├ bin
├ var
├ root
```

2. Important Directories Inside /

Below are the most important folder you must know:

1. /home — User files

- Each user has a seperate folder here.

ex:

/home/gautam

This like "Document" in window

2. /root — Root User's Home

- Special home directory for root (admin) user.
- Normal user cannot access this

3. /etc — Configuration file (very important)

Stores configuration setting for your system and software.

ex:-

- Network settings
- User accounts
- SSH configuration.

This is one of the most important directory for cybersecurit

4. /bin — Basic Commands

Contains essential commands used by all users :

ex: /bin : ls, cp, mv, rm, cat, ping

Without this directory, system cannot work properly.

5. /Sbin - System Commands.

Command used by system administrators :

ex:-

ifconfig reboot shutdown fdisk

Normal users cannot run these without sudo.

6. /usr - User Installed software.

Contains software and libraries installed by the system.

Subdirectories :

- /usr/bin
- /usr/sbin
- /usr/lib Most application you installed live here.

7. /var – Variable Data

Stores files that keep changing

- Logs → /var/log
- Mail
- Cache
- Data bases.

Cybersecurity analysts check log files here.

8. /tmp — temporary files

- Used for temporary storage.
- Gets cleared automatically after reboot.

Helpful during installations.

9. /boot → Boot files.

Contains files needed to boot the system:

- Linux kernel
- GRUB bootloader

ex:

vmlinuz

initrd.img

10. /opt → optional software

Third-party apps are often installed here.

/opt/google

- Login in, switching users, SSH basic

1. Logging In (Local & Remote)

You can log in to linux in two ways:

(A) Logging in Locally (Your own laptop/PC)

1. GUI Login (Graphical)

You type:

- Username
- Password

Then you get desktop

2. Terminal Login (TTY mode)

press Ctrl + Alt + F2 (or F3 ... F6)

login : gautam

password:

after entering password → you get terminal access.

2. Switching Users.

In Linux, you can switch between users using commands.

A) Check current User

whoami

B) Switch to another use

su - username

ex:.

su - jon

Now your terminal become jon's account (if you know password.).

(C) Switch to Root (Admin User)

Root user = full power

sudo su

or

su -

(D) Run only ONE command as root

sudo apt update.

This is safer than becoming full root.

(E) List all users loggen in

who

3. SSH Basic (Secure Shell)

SHH is used to access another computer remotely in a secure way.

Used hevily in cybersecurity, hacking, server administration.

A) SSH Command (very Important)

ssh username @ IP- address

ex:

ssh gautam@ 192.168.1.10

Means:

- Login as gautam
- into remote machine 192.168.1.10

B) SSH Default port

22.

C) SSH using a different Port

ssh -p 2222 username@IP

D) First time Connection Warning

You will see:

Are you sure you want to continue connecting (Yes/No)?

Type:

Yes.

E) SSH Using key Authentiation (More secure)

1. Generate SSH key

ssh-keygen

Keys generated:

- private key → stays with you
- public key → copied to server

2. Copy public key to server.

ssh-copy-id username@server-ip

Now you can login without password.

F. SSH config File (Make login easier)

nano ~/.ssh/config

Add:

Host myserver

Host Name 192.168.1.10

User gautam

Port 22

Now Connect Using :

ssh myserver