A Comprehensive Guide to Essential Linux Commands, Filesystem Navigation, and System Diagnostics

**1. Introduction to Linux Terminal**

**Opening a Terminal in Kali Linux**

* **Shortcut:**
  + **Linux:** Ctrl + Alt + T
  + **Mac:** Ctrl + Option + T (if using SSH)

A screenshot of a computer

AI-generated content may be incorrect.

It defaults to user’s home directory (Here we used pwd – print working directory command in the terminal to display the current directory’s full path)

A close up of a computer screen

AI-generated content may be incorrect.

* **Default Directory:**
  + The terminal opens in the user’s home directory (/home/kali for user "kali").
  + Use pwd (Print Working Directory) to confirm the current path.

**2. Linux Filesystem Hierarchy Standard (FHS)**

Linux follows a standard directory structure defined by the FHS. It specifies where files should be located.

A screenshot of a computer

AI-generated content may be incorrect.

**Linux Filesystem Hierarchy Standard (FHS) - Quick Reference:**

|  |  |  |  |
| --- | --- | --- | --- |
| Directory | Common Name / Purpose | What's Stored Here (Simple Examples) | Analogy / Think Of It Like... |
| **/** | Root Directory | The very top of the entire Linux file system. Everything starts here. | The foundation of a house, or the main trunk of a tree. |
| /bin | User Binaries | Essential basic commands for *all* users (e.g., ls, cp, mv). | Your everyday toolkit (hammer, screwdriver, wrench). |
| /boot | Boot Loader Files | Files needed to start (boot) the Linux operating system. | The engine and starting mechanism of your car. |
| /dev | Devices | Special files representing hardware devices (e.g., hard drives, USB). | Plug-and-play ports and control panels for your computer hardware. |
| /etc | Configuration Files | System-wide configuration files (e.g., network settings, user lists). | The instruction manual and settings panel for the entire house. |
| /home | User Home Directories | Personal files and settings for regular users. | Each person's individual bedroom or private office. |
| /lib | Essential Libraries | Shared code libraries needed by programs in /bin and /sbin. | Common parts (like screws or batteries) that many tools need to work. |
| /lost+found | Recovered Files | Files recovered if the system crashes or shuts down improperly. | The "lost and found" box at school or a public place. |
| /media | Removable Media Mount Point | Where external devices (USB sticks, DVDs) are automatically connected. | The designated parking spot for guest cars. |
| /mnt | Temporary Mount Point | A place for system administrators to temporarily connect other file systems. | A temporary parking spot for a moving truck. |
| /opt | Optional Applications | Large, self-contained third-party software packages. | A dedicated shed for specialized equipment or large projects. |
| /proc | Process Info (Virtual Filesystem) | A virtual view of running processes and system information. Not real files. | A live dashboard showing what's running inside the computer. |
| /root | Root User's Home Directory | The home directory for the "superuser" (administrator). | The system administrator's private office. |
| /run | Runtime Data | Temporary data that changes while the system is running, cleared on reboot. | A whiteboard or notepad for quickly jotting down temporary tasks. |
| /sbin | System Binaries | Essential system administration commands (used by root for maintenance). | The maintenance crew's specialized tools (only they can use them). |
| /srv | Service Data | Data for services offered by the system (e.g., website files). | A public display or service area (like a web server's content). |
| /sys | System Filesystem (Virtual) | A virtual view of connected hardware and kernel settings. | The electrical panel and wiring diagrams for the house's systems. |
| /tmp | Temporary Files | Files created temporarily by programs; often cleared on reboot. | A scrap paper bin or a temporary holding area for junk. |
| /usr | Unix System Resources | Most user-installed programs, libraries, documentation, and shared files. | The main library or software repository. |
| /var | Variable Data Files | Data that changes frequently (e.g., logs, mail queues, website data). | A filing cabinet for ongoing records, logs, and incoming mail. |

Remotely Connected to a linux terminal from a Mac terminal using SSH:

* 1st step: started SSH service on linux terminal by giving command

***Service ssh start*** , then it will ask for user’s authentication, once authenticated .

* 2nd step: ***ssh username@mac\_ip\_address*** (ssh kali@192.18.64.18)
* 3rd step: ***verify*** the host key, type ***yes*** to continue

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Root directory :

A close-up of words

AI-generated content may be incorrect.

The most common commands for navigating the file system are:

**Linux Commands Cheat Sheet:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Command** | **Description** | **Example** |
| **Navigation** | ls | List directory contents | ls -l *(detailed list)* |
|  | cd | Change directory | cd ~/Documents |
|  | pwd | Print working directory | pwd *(shows current path)* |
| **File Management** | mkdir | Create a directory | mkdir new\_folder |
|  | rmdir | Remove **empty** directory | rmdir old\_dir |
|  | rm | Delete files/dirs | rm file.txt rm -rf dir/ *(force delete)* |
|  | cp | Copy files/dirs | cp file.txt backup/ cp -r dir/ backup/ *(recursive)* |
|  | mv | Move/rename files | mv old.txt new.txt mv file.txt ~/Downloads/ |
|  | touch | Create empty file | touch new\_file.txt |
| **Search** | find | Search for files | find /home -name "\*.log" |
|  | grep | Search text in files | grep "error" /var/log/syslog |
|  | locate | Fast file search | locate config.ini *(requires updatedb)* |
| **System Info** | df | Disk space usage | df -h *(human-readable)* |
|  | du | Directory size | du -sh ~/Downloads |
|  | free | Memory usage | free -h |
| **Permissions** | chmod | Change file permissions | chmod 755 script.sh |
|  | chown | Change file owner | sudo chown user:group file.txt |
| **Processes** | ps | List processes | ps aux | grep chrome |
|  | kill | Terminate process | kill -9 1234 *(force kill PID 1234)* |
|  | top | Live process monitor | top *(press q to quit)* |
| **Networking** | ping | Test network connection | ping google.com |
|  | ifconfig | Network interfaces | ifconfig *(or ip a)* |
|  | wget | Download files | wget https://example.com/file.zip |
| **Archives** | tar | Create/extract archives | tar -xvf archive.tar.gz |
|  | zip/unzip | Compress/unzip | zip archive.zip file.txt unzip archive.zip |
| **Text Editing** | nano | Simple text editor | nano file.txt |
|  | cat | Display file content | cat notes.txt |
|  | head/tail | View file start/end | tail -n 20 log.txt *(last 20 lines)* |
| **Package Mgmt** | apt | Debian package manager | sudo apt install nmap |
|  | dnf | RHEL package manager | sudo dnf install git |

cd [directory path]

**cd (Change Directory)**

* **Purpose:** The cd command is used to **change your current working directory**. Think of it as moving between folders on your computer.

 **cd /**

* Changes your current directory to the **root directory** (/), which is the very top of the Linux file system hierarchy.

 **cd ~**

* Changes your current directory to your **home directory**.
  + If you are the kali user, this will take you to /home/kali.
  + If you are the root user, this will take you to /root.

 **cd ..**

* Changes your current directory to the **parent directory** (the directory directly above your current one).
  + If you are in /home/kali/Documents, cd .. will take you to /home/kali.

**cd -**

* Changes your current directory to the **previous directory** you were in. It's like an "undo" for your last cd command.

**cd <directory name>**

* Changes to a subdirectory within your current directory.
  + If you are in /home/kali, cd Documents will take you to /home/kali/Documents.

**cd /path/to/directory**

* Changes to a specific directory using its **absolute path** (starting from /).
  + cd /var/log will take you to the /var/log directory from anywhere.

**cd (by itself)**

* If you type cd with no arguments, it's equivalent to cd ~, meaning it will take you to your home directory.

**pwd (Print Working Directory)**

* **Purpose:** The pwd command is used to **print the absolute path of your current working directory**. It tells you exactly "where you are" in the filesystem hierarchy.

**ls (List Directory Contents)**

* **Purpose:** The ls command is used to **list the contents of a directory**. By default, it lists the contents of your current directory.

**ls -l (Long Listing Format)**

* **Purpose:** Displays directory contents in a **long format**, providing detailed information about each file and directory.
* **-l option:** Stands for "long listing format."

**ls -a (All Files)**

* **Purpose:** Lists all files, including **hidden files** (those whose names start with a dot .).
* **-a option:** Stands for "all."

**ls -la (Long Listing, All Files)**

* **Purpose:** Combines the -l (long format) and -a (all files) options. It provides **detailed information for all files, including hidden ones.**
* **-la option:** A common and very useful combination.

**ls -lah (Long Listing, All Files, Human-Readable Size)**

* **Purpose:** Adds the -h option to ls -la, making file sizes easier to read.
* **-h option:** Stands for "human-readable." It converts byte sizes into K (kilobytes), M (megabytes), G (gigabytes), etc.

A screenshot of a computer

AI-generated content may be incorrect.

A white background with blue text

AI-generated content may be incorrect.

**Key Notes:**

1. **Flags Matter**:
   * -r = recursive (for directories)
   * -f = force (bypass prompts)
   * -h = human-readable (e.g., df -h)
2. **Admin Rights**: Use sudo before commands requiring root access (e.g., sudo apt update).
3. **Wildcards**:
   * \* = match any characters (e.g., rm \*.tmp)
   * ? = match single character (e.g., ls file?.txt)
4. **Shortcuts**:
   * Ctrl+C = Kill current process
   * Ctrl+Z = Suspend process
   * !! = Repeat last command

**Linux Process & Service Management Commands:**

|  |  |  |
| --- | --- | --- |
| **Command** | **Description** | **Example** |
| ps aux | List all running processes | ps aux | grep chrome *(Find Chrome processes)* |
| top or htop | Interactive process monitor | htop *(Press F10 to exit)* |
| kill <PID> | Terminate a process by ID | kill 1234 *(Graceful termination)* |
| kill -9 <PID> | Force kill a process | kill -9 1234 *(Immediate termination)* |
| nice -n <priority> <cmd> | Start process with custom priority | nice -n 10 ./script.sh *(Lower priority)* |
| renice -n <priority> -p <PID> | Change priority of running process | renice -n 5 -p 1234 \*(New priority=5)\* |
| jobs | List background jobs | jobs -l *(Show job IDs and PIDs)* |
| bg %<job\_id> | Resume job in background | bg %1 *(Resume job ID 1)* |
| fg %<job\_id> | Bring job to foreground | fg %2 *(Bring job ID 2 to foreground)* |

**System Services (systemd):**

|  |  |  |
| --- | --- | --- |
| **Command** | **Description** | **Example** |
| systemctl start <service> | Start a service | sudo systemctl start nginx |
| systemctl stop <service> | Stop a service | sudo systemctl stop apache2 |
| systemctl restart <service> | Restart a service | sudo systemctl restart ssh |
| systemctl status <service> | Check service status | systemctl status mysql *(View live status)* |
| systemctl enable <service> | Enable service at boot | sudo systemctl enable docker |
| systemctl disable <service> | Disable service at boot | sudo systemctl disable postgresql |
| systemctl list-units --type=service | List all services | systemctl list-units --type=service |
| journalctl -u <service> | View service logs | journalctl -u nginx --since today |

**Linux Account Management Cheat Sheet:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Command** | **Description** | **Example** |
| **User Management** | useradd <username> | Create new user account | sudo useradd kishore |
|  | passwd <username> | Set/change user password | sudo passwd kishore |
|  | userdel -r <username> | Delete user and home directory | sudo userdel -r kishore |
|  | usermod <options> <username> | Modify user account | sudo usermod -s /bin/zsh kishore |
| **Group Management** | groupadd <groupname> | Create new group | sudo groupadd developers |
|  | groupdel <groupname> | Delete group | sudo groupdel developers |
|  | usermod -aG <group> <user> | Add user to group | sudo usermod -aG developers kishore |
|  | gpasswd -d <user> <group> | Remove user from group | sudo gpasswd -d kishore developers |
| **Account Info** | id <username> | Show user UID, GID, and groups | id kishore |
|  | getent passwd <username> | Display user account info | getent passwd kishore |
|  | groups <username> | List user's groups | groups kishore |
| **Password Control** | chage -l <username> | Show password aging info | sudo chage -l kishore |
|  | passwd -e <username> | Force password change on next login | sudo passwd -e kishore |
|  | passwd -l <username> | Lock user account | sudo passwd -l kishore |
|  | passwd -u <username> | Unlock user account | sudo passwd -u kishore |

**Key Account Configuration Files:**

|  |  |  |
| --- | --- | --- |
| **File Path** | **Contents** | **Access** |
| /etc/passwd | User accounts (UID, GID, home dir, shell) | Readable by all |
| /etc/shadow | Encrypted passwords and aging info | Root only |
| /etc/group | Group definitions and members | Readable by all |
| /etc/gshadow | Secure group passwords and administrators | Root only |
| /etc/skel/ | Default files for new user home directories | Root/managers |
| /etc/login.defs | Password aging and user creation defaults | Root only |
| /etc/default/useradd | Default settings for new users | Root only |

**Advanced Commands:**

|  |  |  |
| --- | --- | --- |
| **Command** | **Purpose** | **Example** |
| newusers <filename> | Batch create users from file | sudo newusers userlist.txt |
| chage <options> <username> | Modify password expiration | sudo chage -M 90 kishore |
| pwck | Verify password file integrity | sudo pwck |
| grpck | Verify group file integrity | sudo grpck |
| vigr | Safely edit /etc/group file | sudo vigr |
| vipw | Safely edit /etc/passwd file | sudo vipw |

**Always use**sudo for account modifications

**Linux File Permissions Master Table:**

**Basic Permissions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Symbol** | **Numeric** | **User Type** | **File Effect** | **Directory Effect** | **Example Command** |
| r (read) | 4 | Owner (u) | View content | List files | chmod u+r file.txt |
|  |  | Group (g) |  |  | chmod g+r /shared/ |
|  |  | Others (o) |  |  | chmod o+r public.log |
| w (write) | 2 | Owner | Modify content | Create/delete files | chmod u+w script.sh |
|  |  | Group |  |  | chmod g+w /team\_data/ |
|  |  | Others |  |  | chmod o+w temp/ |
| x (execute) | 1 | Owner | Run as program | Enter directory | chmod u+x backup.sh |
|  |  | Group |  |  | chmod g+x /projects/ |
|  |  | Others |  |  | chmod o+x /public\_bin/ |

**Common Combinations:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Mode** | **Symbolic** | **Owner** | **Group** | **Others** | **Typical Use** |
| 755 | rwxr-xr-x | Read+Write+Execute | Read+Execute | Read+Execute | Scripts, programs |
| 644 | rw-r--r-- | Read+Write | Read | Read | Config files |
| 700 | rwx------ | Full access | No access | No access | Private directories |

**Special Permissions**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Permission** | **Symbol** | **Numeric** | **Effect** | **Example** |
| **SetUID** | s | 4000 | Runs as file owner | chmod 4755 /usr/bin/passwd |
| **SetGID** | s | 2000 | Runs with file's group OR new files inherit directory's group | chmod 2755 /shared/ |
| **Sticky Bit** | t | 1000 | Only owner can delete files | chmod 1777 /tmp/ |

**ACL (Advanced Permissions)**

|  |  |  |
| --- | --- | --- |
| **Command** | **Effect** | **Example** |
| setfacl -m u:user:perms file | Grant user-specific permissions | setfacl -m u:kishore:rwx project.txt |
| setfacl -m g:group:perms file | Grant group-specific permissions | setfacl -m g:devs:r-- config.cfg |
| setfacl -x u:user file | Remove user's ACL entry | setfacl -x u:tempuser report.pdf |
| getfacl file | View all ACLs | getfacl /shared/docs/ |

**ACL Permission Types:**

|  |  |
| --- | --- |
| **Shortcut** | **Meaning** |
| r | Read |
| w | Write |
| x | Execute |
| - | No permission |

**Linux Storage & Filesystem Diagnostic Tools for Cybersecurity:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Command** | **Effect** | **Example** | **Cybersecurity Use Case** |
| df -h | Show disk usage in human-readable format (GB/MB) | df -h /home | Detect unexpected disk full conditions (possible log poisoning attack) |
| du -sh /dir | Calculate total space used by a directory | du -sh /var/log | Identify abnormally large log directories (indicator of attack activity) |
| find / -type f -size +1G | Locate files larger than 1GB | find /home -type f -size +500M | Hunt for exfiltrated data or malware binaries |
| iostat | Monitor I/O performance (CPU, device utilization) | iostat -x 2 | Detect crypto-mining malware or ransomware encrypting files |
| lsblk | List block devices and mount points | lsblk -f | Verify unauthorized storage devices or encrypted partitions |
| blkid | Show UUIDs and filesystem types of block devices | blkid /dev/sda1 | Verify device integrity (compare against known good UUIDs) |
| mount**/**umount | Mount/unmount filesystems | mount /dev/sdb1 /mnt/forensics | Secure evidence collection during investigations |
| cat /proc/mdstat | Check software RAID status and synchronization | cat /proc/mdstat | Verify RAID integrity after suspected hardware tampering |
| lvs | List Logical Volumes (LVM) | lvs --all | Audit LVM configurations for security hardening |
| vgs | List Volume Groups (LVM) | vgs -v | Check for unauthorized volume groups |
| pvs | List Physical Volumes (LVM) | pvs --segments | Verify physical disk allocations in enterprise environments |