Advanced Linux Commands Cheat Sheet

Created by UbuntuFree.com

This cheat sheet covers essential and advanced Linux commands for system management, security, networking, and user control. Each command is explained in plain English, with practical examples to help you understand when and how to use them effectively.

1. sudo : Run Commands as Superuser

Use `sudo` to execute commands with administrative (root) privileges.

```
sudo apt update
```

Example: Update your system's package list.

2. ssh : Secure Remote Login

Connect securely to a remote machine via SSH (Secure Shell).

```
ssh user@192.168.1.100
```

Example: Log into a remote server using SSH keys instead of passwords for added security.

3. scp : Secure File Copy

Copy files securely between your local machine and a remote system.

```
scp file.txt user@192.168.1.100:/home/user/
```

Example: Upload a file to a remote server.

4. sftp : Secure File Transfer Protocol

Transfer files securely using the interactive SFTP shell.

```
sftp user@192.168.1.100
```

Example: Start a secure file transfer session to a remote server.

5. iptables : Manage Firewall Rules

Configure advanced firewall rules to control incoming and outgoing network traffic.

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

Example: Allow SSH connections on port 22.

6. ufw : Uncomplicated Firewall

A user-friendly interface for managing iptables firewall rules.

```
sudo ufw enable
sudo ufw allow 80/tcp
```

Example: Enable the firewall and allow HTTP traffic.

7. fail2ban : Block Malicious IPs

Monitors log files and bans IPs showing suspicious behavior like brute-force attacks.

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

Example: Check the status of the SSH jail.

8. nmap : Network Port Scanner

Scan your network or server for open ports and services.

```
nmap -sV 192.168.1.100
```

Example: Detect open ports and running services on a target machine.

9. chmod : Change File Permissions

Modify read, write, and execute permissions for files or directories.

```
chmod 755 myscript.sh
```

Example: Give owner full rights and read/execute to others.

10. chown : Change File Ownership

Change the owner and group of a file or directory.

```
sudo chown user:user /var/www/html
```

Example: Assign a web directory to the correct user.

11. chkrootkit : Rootkit Detection

Scan your system for known rootkits.

```
sudo chkrootkit
```

Example: Run a system-wide rootkit check.

12. rkhunter : Rootkit Scanner

Checks for rootkits, backdoors, and local exploits.

```
sudo rkhunter --check
```

Example: Perform a detailed rootkit scan.

13. lynis : Security Auditing Tool

Performs a full security audit of your Linux system.

```
sudo lynis audit system
```

Example: Generate a comprehensive security report.

14. openssl : Cryptographic Toolkit

Encrypt data, manage SSL certificates, and more.

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

Example: Encrypt a file using AES-256.

15. gpg : File & Email Encryption

Encrypt files or sign emails with GNU Privacy Guard.

```
gpg -c confidential.txt
```

Example: Encrypt a sensitive file.

16. passwd : Change User Password

Allows a user to change their own password.

```
passwd
```

Example: Prompt to set a new password for the current user.

17. chpasswd : Batch Password Update

Update passwords for multiple users at once.

```
echo "john:newpassword" | sudo chpasswd
```

Example: Change the password for user "john".

18. chroot : Change Root Directory

Run a command or shell within a different root directory (often for isolation).

```
sudo chroot /mnt/recovery
```

Example: Enter a chroot environment for system recovery.

19. su : Switch User

Switch to another user account within the terminal.

```
su - username
```

Example: Become another user without logging out.

20. selinux : Security-Enhanced Linux

Manage and enforce access control policies on RedHat-based systems.

```
getenforce
```

Example: Check the current SELinux status.

21. firewalld : Dynamic Firewall Manager

Manages firewall rules dynamically with support for zones.

```
sudo firewall-cmd --zone=public --add-port=8080/tcp
```

Example: Open port 8080 on the public zone.

22. auditd : Audit Daemon

Logs system events for security auditing and incident investigation.

```
sudo service auditd status
```

Example: Check if the audit service is active.

23. logwatch : Log Analyzer

Analyzes and summarizes log files.

```
sudo logwatch --detail High --service sshd --range today
```

Example: Generate a detailed report on SSHD activity.

24. tripwire : File Integrity Checker

Monitors file integrity to detect unauthorized changes.

```
sudo tripwire --check
```

Example: Run a system-wide file integrity check.

25. apparmor : Application Armor

Restrict applications' access to system resources with mandatory access control profiles.

```
sudo aa-status
```

Example: View current AppArmor profile statuses.

26. OpenSCAP : Compliance & Hardening

Automates security compliance checks and system hardening.

```
oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_pci-dss /usr/share/xml/scap/ssg/content/ssg-ubuntu1804-ds.xml
```

Example: Run a PCI-DSS compliance scan.

27. AIDE : Advanced Intrusion Detection Environment

Monitors system files and directories for unauthorized changes.

```
sudo aide --check
```

Example: Verify if any critical files have been modified.