

[Created for free by UbuntuFree.com](https://www.ubuntufree.com/)

Linux Security Commands Cheat Sheet

Keep this cheat sheet handy to strengthen your Linux system's security. Below are 15 essential commands you should master to manage user access, monitor activity, and secure your server.

Critical Security Commands Explained

1. passwd

Change the password of the current user.

passwd

2. chown

Change ownership of a file or directory.

sudo chown user:group filename

3. chmod

Modify file or directory permissions.

chmod 755 filename

4. su

Switch to another user account.

su - username

5. sudo

Execute a command as the superuser or another user.

sudo command

6. ssh

Establish a secure shell connection to a remote server.

ssh user@hostname

7. scp

Securely copy files between systems.

scp file.txt user@remote:/path/

8. ufw

Manage firewall rules easily.

sudo ufw enable

9. iptables

Configure advanced firewall rules.

sudo iptables -L

10. fail2ban

Monitor log files and ban suspicious IPs.

sudo fail2ban-client status

11. netstat

Display active network connections.

netstat -tuln

12. nmap

Scan open ports on a system.

nmap 192.168.1.1

13. rkhunter

Scan for rootkits on your system.

sudo rkhunter --check

14. auditd

Audit and monitor system activity.

sudo systemctl status auditd

15. openssl

Generate SSL certificates and manage encryption.

openssl genrsa -out private.key 2048

Other Useful Security Commands (Quick Reference)

Command Description

chpasswd Change passwords of multiple users at once

chroot Create a restricted virtual environment

sftp Secure File Transfer Protocol

lynis Perform security audits and vulnerability scans

snort Network Intrusion Detection System (NIDS)

gpg Encrypt and sign files/emails using GnuPG

firewalld Advanced firewall management with zones

selinux Mandatory Access Control (MAC) for Linux

chkrootkit Scan for rootkits

logwatch Analyze logs and generate reports

tripwire Monitor file integrity changes

apparmor Restrict program capabilities via profiles

OpenSCAP System hardening and compliance checking

AIDE Advanced Intrusion Detection Environment