



50 Essential Kali Linux Commands

A comprehensive guide to
system, networking, and
security commands.



Basic System Commands

- **uname -a:** Displays system information, including kernel version and architecture.
- **lsb_release -a:** Shows detailed information about the Kali Linux version.
- **pwd:** Prints the current working directory.
- **ls -lah:** Lists all files, including hidden ones, with details.
- **cd /path/to/folder:** Changes the current directory to a specified folder.

Basic System Commands

- **cp file1 file2:** Copies a file from one location to another.
- **mv file1 file2:** Moves or renames a file.
- **rm -rf folder:** Deletes a folder and its contents.
- **find / -name filename:** Searches for a file named 'filename' in the system.
- **grep 'text' file.txt:** Searches for specific text inside a file.

User Management & Permissions

- **whoami**: Shows the current logged-in user.
- **id**: Displays user ID (UID) and group ID (GID).
- **passwd**: Changes the password of the current user.
- **chmod 755 file**: Changes file permissions.
- **chown user:group file**: Changes the ownership of a file.
- **adduser username**: Adds a new user to the system.

User Management & Permissions

- **deluser username:** Removes a user from the system.
- **su - username:** Switches to another user account.
- **groups:** Displays the groups the current user belongs to.
- **usermod -aG sudo username:** Adds a user to the sudo (admin) group.

Networking Commands

- **ifconfig**: Displays network interfaces and IP addresses.
- **ip a**: Shows detailed IP address and network interface details.
- **ping google.com**: Tests network connectivity by sending packets.
- **netstat -tulnp**: Shows open ports and running services.
- **nmap -sS target_ip**: Performs a stealth scan on a target IP.
- **arp -a**: Displays the ARP table (connected devices).

Networking Commands

- **traceroute google.com:** Shows the route packets take to reach a destination.
- **wget url:** Downloads a file from the internet.
- **curl -I google.com:** Fetches HTTP headers of a website.
- **airmon-ng start wlan0:** Enables monitor mode on a wireless interface.

Process Management

- **ps aux:** Lists all running processes.
- **top:** Shows real-time CPU and memory usage.
- **htop:** An enhanced version of top for interactive process management.
- **kill -9 process_id:** Forces termination of a specific process.
- **pkill process_name:** Kills a process by its name.

Process Management

- **service apache2 start:** Starts the Apache web server service.
- **service apache2 stop:** Stops the Apache web server service.
- **systemctl restart networking:** Restarts the networking service.
- **crontab -e:** Opens the cron job scheduler for automating tasks.
- **journalctl -xe:** Displays system logs for troubleshooting

Security & Ethical Hacking Tools

- **msfconsole**: Launches the Metasploit Framework for penetration testing.
- **hydra -l user -P passlist.txt target**: Performs brute-force login attempts.
- **john --wordlist=rockyou.txt hash.txt**: Uses John the Ripper to crack password hashes.
- **sqlmap -u 'http://target.com/index.php?id=1' --dbs**: Tests for SQL Injection vulnerabilities.
- **nikto -h target.com**: Scans a website for security vulnerabilities.

Security & Ethical Hacking Tools

- **hashcat -m 0 -a 3 hash.txt ?a?a?a?a:** Cracks password hashes using Hashcat.
- **wireshark:** Starts Wireshark for network packet analysis.
- **dirb http://target.com/:** Performs directory brute-forcing on a website.
- **setoolkit:** Opens the Social Engineering Toolkit for phishing attacks.
- **maltego:** Launches Maltego, an OSINT tool for intelligence gathering.