

Kali Linux Command Cheat Sheet

Quick reference • Terminal basics • Networking • Security tools

How to use: Open Terminal (usually Ctrl+Alt+T). Replace placeholders such as <interface> or <target> with your own values. Commands are case-sensitive. Kali is Debian-based, so many standard Linux commands and APT package commands also apply.

1. Help and command basics

Command	What it does	Example
man <command>	Open the manual page for a command.	man nmap
<command> --help	Display command-line help.	nmap --help
apropos <keyword>	Search manual-page descriptions by keyword.	apropos network
which <command>	Show the executable path found in PATH.	which python3
type <command>	Show how the shell interprets a command.	type ls
history	List commands entered in the current shell.	history
clear	Clear the terminal display.	clear

2. Files and directories

Command	What it does	Example
pwd	Print the current working directory.	pwd
ls -lah	List files, including hidden files, with details and readable sizes.	ls -lah
cd <directory>	Change directory.	cd /usr/share
cd ..	Move up one directory.	cd ..
cd ~	Go to your home directory.	cd ~
mkdir -p <path>	Create directories, including missing parent directories.	mkdir -p labs/reports
touch <file>	Create an empty file or update its timestamp.	touch notes.txt
cp <source> <destination>	Copy a file.	cp notes.txt notes-copy.txt
cp -r <source> <destination>	Copy a directory recursively.	cp -r lab lab-backup
mv <source> <destination>	Move or rename a file/directory.	mv draft.txt final.txt
rm <file>	Delete a file; deletion may be difficult to reverse.	rm temporary.txt
file <path>	Identify the type of a file.	file sample.bin

3. Reading, searching and editing

Command	What it does	Example
cat <file>	Print a file's contents.	cat notes.txt
less <file>	Read a file page by page; press q to quit.	less /var/log/auth.log
head -n 20 <file>	Show the first 20 lines.	head -n 20 scan.txt
tail -n 20 <file>	Show the last 20 lines.	tail -n 20 scan.txt
tail -f <file>	Follow new lines appended to a log.	tail -f /var/log/syslog
grep -in '<text>' <file>	Search case-insensitively and show line numbers.	grep -in 'failed' auth.log
grep -R '<text>' <dir>	Search recursively in files under a directory.	grep -R 'TODO' ./scripts
find <dir> -name '<pattern>'	Find files by name.	find . -name '*.pcap'

Command	What it does	Example
locate <name>	Search the locate database; database may need updating.	locate rockyou.txt
nano <file>	Edit a text file in a simple terminal editor.	nano notes.txt

4. Permissions and privilege

Command	What it does	Example
ls -l <path>	View file permissions, owner and group.	ls -l script.sh
chmod +x <file>	Add executable permission where applicable.	chmod +x script.sh
chmod 600 <file>	Give owner read/write; remove group/other access.	chmod 600 private.key
chmod 644 <file>	Owner read/write; others read.	chmod 644 notes.txt
chown <user>:<group> <path>	Change ownership; normally requires elevated privileges.	sudo chown user:user notes.txt
sudo <command>	Run a command with elevated privileges when authorised.	sudo apt update
id	Show your user and group IDs.	id
whoami	Print the current username.	whoami
sudo -l	Show commands your account may run through sudo.	sudo -l

5. APT packages and Kali updates

Command	What it does	Example
sudo apt update	Refresh package index information.	sudo apt update
sudo apt full-upgrade	Upgrade packages and handle dependency changes.	sudo apt full-upgrade
sudo apt install <package>	Install a package from configured repositories.	sudo apt install nmap
sudo apt remove <package>	Remove a package.	sudo apt remove package-name
sudo apt autoremove	Remove dependencies no longer required.	sudo apt autoremove
apt search <term>	Search available packages.	apt search wireshark
apt show <package>	Show package details.	apt show sqlmap
dpkg -l	List installed packages.	dpkg -l less
kali-tweaks	Open Kali's configuration utility, if installed.	kali-tweaks

6. System information, processes and services

Command	What it does	Example
uname -a	Show kernel and system details.	uname -a
cat /etc/os-release	Show operating-system release information.	cat /etc/os-release
hostnamectl	Show hostname and related system information.	hostnamectl
uptime	Show uptime and load averages.	uptime
free -h	Show memory and swap usage.	free -h
df -h	Show filesystem disk space.	df -h
du -sh <path>	Show total disk usage for a path.	du -sh ~/Downloads
ps aux	List running processes.	ps aux
top	Interactively monitor processes and resource use.	top
kill <PID>	Request a process to terminate.	kill 1234
systemctl status <service>	Check a systemd service's status.	systemctl status NetworkManager

Command	What it does	Example
<code>journalctl -b</code>	View logs from the current boot.	<code>journalctl -b</code>

7. Networking and connectivity

Command	What it does	Example
<code>ip addr</code>	Show network interfaces and IP addresses.	<code>ip addr</code>
<code>ip route</code>	Show routing table and default route.	<code>ip route</code>
<code>ip link</code>	Show network interfaces and link state.	<code>ip link</code>
<code>ping -c 4 <host></code>	Test reachability and latency; ping may be blocked.	<code>ping -c 4 1.1.1.1</code>
<code>ss -tulpn</code>	List listening TCP/UDP sockets; process details may need sudo.	<code>sudo ss -tulpn</code>
<code>ip neigh</code>	Show the local neighbour/ARP table.	<code>ip neigh</code>
<code>curl -I <URL></code>	Request HTTP headers from a URL.	<code>curl -I https://example.com</code>
<code>wget <URL></code>	Download a resource from a URL.	<code>wget https://example.com/file.txt</code>
<code>dig <domain></code>	Query DNS records; may require dnsutils.	<code>dig example.com</code>
<code>traceroute <host></code>	Trace the network path; may require installation.	<code>traceroute example.com</code>
<code>nmcli device status</code>	Show NetworkManager device status.	<code>nmcli device status</code>

8. Security and network assessment tools

Command	What it does	Example
<code>nmap -h</code>	Display Nmap help and options.	<code>nmap -h</code>
<code>nmap -sn <authorised-subnet></code>	Discover responding hosts without a port scan.	<code>nmap -sn 192.0.2.0/24</code>
<code>nmap -sV <authorised-target></code>	Probe open ports to identify service/version information.	<code>nmap -sV 192.0.2.10</code>
<code>nmap -O <authorised-target></code>	Attempt operating-system detection; may need elevated privileges.	<code>sudo nmap -O 192.0.2.10</code>
<code>wireshark</code>	Launch the graphical packet-analysis application, if installed.	<code>wireshark</code>
<code>tshark -r <capture.pcap></code>	Read and dissect packets from a capture file.	<code>tshark -r traffic.pcap</code>
<code>tcpdump -i <interface></code>	Capture packets on a selected interface; may need sudo.	<code>sudo tcpdump -i eth0</code>
<code>sha256sum <file></code>	Calculate a SHA-256 checksum for integrity checking.	<code>sha256sum evidence.zip</code>
<code>gpg --verify <signature> <file></code>	Verify a signed file when the correct signature/key is available.	<code>gpg --verify file.sig file</code>
<code>searchsploit <term></code>	Search the local Exploit-DB index, if installed.	<code>searchsploit apache 2.4</code>
<code>msfconsole</code>	Launch Metasploit Framework, if installed; use only in authorised labs.	<code>msfconsole</code>

9. Web testing and lab utilities

Command	What it does	Example
<code>curl -sS <URL></code>	Fetch a URL and display the response body.	<code>curl -sS https://example.com</code>
<code>whatweb <URL></code>	Identify web technologies; use only on authorised targets.	<code>whatweb https://lab.example</code>
<code>nikto -h <authorised-URL></code>	Run a web-server assessment; noisy and should be authorised.	<code>nikto -h http://192.0.2.10</code>
<code>sqlmap -h</code>	Display sqlmap help; do not test systems without permission.	<code>sqlmap -h</code>
<code>burpsuite</code>	Launch Burp Suite if installed; commonly used for web security testing.	<code>burpsuite</code>
<code>python3 -m http.server 8000</code>	Start a simple HTTP server in the current directory for a local lab.	<code>python3 -m http.server 8000</code>
<code>nc -lvp <port></code>	Listen on a TCP port with netcat variants that support these flags.	<code>nc -lvp 4444</code>

10. Archives and evidence handling

Command	What it does	Example
<code>tar -czf <archive>.tar.gz <path></code>	Create a gzip-compressed tar archive.	<code>tar -czf lab-backup.tar.gz lab/</code>
<code>tar -xzf <archive>.tar.gz</code>	Extract a gzip-compressed tar archive.	<code>tar -xzf lab-backup.tar.gz</code>
<code>tar -tf <archive>.tar.gz</code>	List archive contents without extracting.	<code>tar -tf lab-backup.tar.gz</code>
<code>zip -r <archive>.zip <dir></code>	Create a ZIP archive; zip may need installing.	<code>zip -r evidence.zip evidence/</code>
<code>unzip <archive>.zip</code>	Extract a ZIP archive.	<code>unzip evidence.zip</code>
<code>sha256sum <file></code>	Record a file's hash for later integrity comparison.	<code>sha256sum capture.pcap</code>
<code>stat <file></code>	Show file size, permissions and timestamps.	<code>stat capture.pcap</code>
<code>cp --preserve=all <src> <dest></code>	Copy while preserving available metadata; not a substitute for forensic imaging.	<code>cp --preserve=all image.dd image-copy.dd</code>

11. Shell operators and shortcuts

Command	What it does	Example
<code>command1 && command2</code>	Run the second command only if the first succeeds.	<code>sudo apt update && sudo apt full-upgrade</code>
<code>command1 ; command2</code>	Run the second command regardless of the first result.	<code>date ; whoami</code>
<code>command1 command2</code>	Pipe output from one command into another.	<code>ps aux less</code>
<code>command > file</code>	Redirect output, replacing the file contents.	<code>ip addr > network.txt</code>
<code>command >> file</code>	Append output to a file.	<code>date >> activity.log</code>
<code>command 2> errors.txt</code>	Redirect standard error to a file.	<code>find / -name test 2> errors.txt</code>
<code>Ctrl+C</code>	Interrupt the foreground command.	—
<code>Ctrl+Z</code>	Suspend the foreground process in many shells.	—
<code>Tab</code>	Autocomplete commands and paths.	—
<code>↑ / ↓</code>	Browse command history.	—

12. Safety, authorisation and good practice

Command	What it does	Example
<code>history</code>	Review recent commands before repeating them.	<code>history</code>
<code>man <command></code>	Read documentation before using unfamiliar options.	<code>man tcpdump</code>
<code>sudo -l</code>	Review your permitted sudo commands.	<code>sudo -l</code>
<code>sha256sum <file></code>	Create a hash to help verify file integrity.	<code>sha256sum evidence.img</code>
<code>script <file></code>	Record a terminal session to a typescript file.	<code>script terminal-session.txt</code>
<code>exit</code>	Close the current shell/session.	<code>exit</code>

Important cautions

- Only scan, test or intercept systems you own or have explicit permission to assess. Use isolated training labs (such as intentionally vulnerable VMs) when learning security tools.
- Network discovery and web-testing tools can generate alerts, affect availability or violate laws/policies if used without authorisation.
- Avoid running unfamiliar commands as root. Commands that delete files, change permissions, capture traffic or modify services can have significant consequences.

- Kali is a rolling distribution. Tool availability, flags and package names may change; check each tool's --help or manual page.
- Examples using 192.0.2.0/24 are documentation-only example addresses, not a real target network.

Prepared as a practical reference for Kali Linux learners and authorised security labs.