Kali Linux Cheat Sheet

Beginner Edition – Hackberry Pi CM5

1 – Getting Oriented on Your Hackberry Pi

Your Hackberry Pi CM5 runs a Cortex-A76 quad-core ARM SoC at 2.4 GHz with up to 16 GB RAM. Kali runs natively on it – the same tools, the same kernel, just on ARM64 instead of x86. The BlackBerry keyboard is great for quick commands once you learn a few shortcuts, but for longer sessions plug in a USB keyboard via one of the two USB 3.0 ports.

First Things First

`sudo apt update && sudo apt upgrade -y`	Update everything. Do this first, always.
`uname -a`	Show kernel version and architecture (aarch64).
`cat /etc/os-release`	Confirm you're on Kali and which version.
`free -h`	Check RAM – know what you're working with.
`df -h`	Disk space. Important if booting from SD.
`lsblk`	List block devices – see your SD, NVMe, USB drives.
`lsusb`	List USB devices (WiFi adapters, SDRs, etc.).
`ip a`	Show network interfaces and IP addresses.
`vcgencmd measure_temp`	Check CPU temp – the aluminium case helps, but monitor it.

Tip: If you put an NVMe SSD in the M.2 slot and boot from it, everything will feel significantly faster than microSD.

2 – Navigating the Filesystem

`pwd`	Print working directory – where am I?
`ls -la`	List everything including hidden files, with permissions.
`cd /path/to/dir`	Change directory. **cd ~** goes home, **cd -** goes back.
`mkdir -p projects/lab1`	Create nested directories in one shot.
`cp -r src/ dst/`	Copy recursively.
`mv old new`	Move or rename.
`rm -rf dir/`	Delete recursively. **No undo.** Be careful.
`find / -name '*.conf' 2>/dev/null`	Search the whole system for .conf files.
`locate filename`	Fast search using a pre-built index (run **updatedb** first).
`tree -L 2`	Visual directory tree, 2 levels deep.

Tip: Tab-completion is your best friend. Type the first few letters and hit Tab.

3 – Reading & Editing Files

`cat file.txt`	Dump entire file to screen.
`less file.txt`	Page through a file. Press **q** to quit.
`head -n 20 file.txt`	First 20 lines.
`tail -n 20 file.txt`	Last 20 lines.

`tail -f /var/log/syslog`	Live-follow a log file – great for debugging.
`grep -ri 'password' /etc/`	Recursively search for a string, case-insensitive.
`nano file.txt`	Beginner-friendly text editor. Ctrl+O saves, Ctrl+X exits.
`vim file.txt`	Powerful editor. Press **i** to type, **Esc** then **:wq** to save & quit.

Tip: Start with nano. Learn vim later when you're comfortable. Don't let anyone gatekeep you on editor choice.

4 – Permissions & Users

Linux permissions matter. Every file has an owner, a group, and a mode (read/write/execute for owner, group, others). The format **rwxr-xr--** means: owner can read/write/execute, group can read/execute, others can only read.

`chmod 750 script.sh`	Owner: rwx, Group: r-x, Others: none.
`chmod u+x script.sh`	Make executable for owner only.
`chown user:group file`	Change ownership.
`whoami`	Who are you logged in as?
`id`	Your user ID, group memberships.
`sudo command`	Run a command as root.
`sudo -s`	Drop into a root shell. Use sparingly.
`passwd`	Change your password.
`adduser newuser`	Create a new user.

Kali defaults to a single user. For real work, create a non-root user and use sudo.

5 – Processes & System Management

`htop`	Interactive process viewer. Better than top.
`ps aux`	Snapshot of all running processes.
`ps aux | grep nmap`	Find a specific process.
`kill PID`	Gracefully stop a process.
`kill -9 PID`	Force-kill a stubborn process.
`systemctl status ssh`	Check if the SSH service is running.
`systemctl start ssh`	Start the SSH daemon.
`systemctl enable ssh`	Auto-start SSH on boot.
`journalctl -xe`	Read system logs when something goes wrong.
`dmesg | tail -30`	Kernel messages – useful for hardware/driver issues.

Tip: If the Hackberry feels sluggish, run htop and look for runaway processes eating CPU or RAM.

6 – Networking Basics

The CM5 has onboard WiFi, but the aluminium case can attenuate the signal. Consider the external FPC antenna mod documented in the Hackberry GitHub repo, or plug in a USB WiFi adapter (one of the USB 3.0 ports).

`ip a`	Show all interfaces and IPs.
`ip link set wlan0 up`	Bring a wireless interface up.
`iwconfig`	Show wireless interface details.

`nmcli dev wifi list`	Scan for WiFi networks.
`nmcli dev wifi connect SSID password PASS`	Connect to a WiFi network.
`ping -c 4 1.1.1.1`	Test connectivity (4 pings).
`traceroute 8.8.8.8`	Trace the route packets take.
`ss -tlnp`	Show listening TCP ports and which process owns them.
`curl ifconfig.me`	What's my public IP?
`wget https://example.com/file.zip`	Download a file.

7 – Package Management (APT)

`sudo apt update`	Refresh the package index.
`sudo apt upgrade -y`	Upgrade all installed packages.
`sudo apt install nmap`	Install a package.
`sudo apt remove nmap`	Remove a package (keeps config).
`sudo apt purge nmap`	Remove package AND config files.
`sudo apt autoremove`	Clean up orphaned dependencies.
`apt search keyword`	Search for packages.
`apt show nmap`	Show info about a package.
`dpkg -l | grep nmap`	Check if something is installed.

8 – Kali Security Tools (Starter Kit)

Kali ships with hundreds of security tools. Here are the ones worth learning first. **Only use these on networks and systems you own or have written permission to test.**

Reconnaissance & Scanning

`nmap -sn 192.168.1.0/24`	Ping sweep – discover live hosts on your LAN.
`nmap -sV -sC target`	Service version detection + default scripts.
`nmap -A -T4 target`	Aggressive scan: OS detection, versions, scripts, traceroute.
`nmap -p- target`	Scan ALL 65535 ports (slow but thorough).
`whois domain.com`	Domain registration info.
`dig domain.com`	DNS lookup.
`nikto -h http://target`	Web server vulnerability scanner.

WiFi (Your Own Network Only)

`airmon-ng`	List wireless interfaces.
`airmon-ng start wlan0`	Put interface into monitor mode.
`airodump-ng wlan0mon`	Capture nearby WiFi traffic – see SSIDs, clients.
`airodump-ng -c 6 --bssid AA:BB:... wlan0mon`	Focus capture on one AP.

Tip: The Pi's onboard WiFi supports monitor mode with nexmon drivers (pre-installed on Kali ARM). A USB adapter like the Alfa AWUS036ACH gives better range and dual-band support.

Web Application Testing

`burpsuite`	Launch Burp Suite – HTTP intercepting proxy.
`gobuster dir -u http://target -w /usr/share/wordlists/dirb/common.txt`	Directory brute-force.
`sqlmap -u 'http://target?id=1' --dbs`	Test for SQL injection.
`wpscan --url http://target`	WordPress vulnerability scanner.

Password & Hash Tools

`john hashfile.txt`	John the Ripper – crack password hashes.
`hashcat -m 0 hash.txt wordlist.txt`	GPU-accelerated cracking (CPU-only on Pi).
`hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://target`	Brute-force SSH login.

Tip: Unzip rockyou first – sudo gunzip /usr/share/wordlists/rockyou.txt.gz

9 – Shell Productivity

`history`	Show command history.
`!!`	Re-run the last command. **sudo !!** is a lifesaver.
`Ctrl+R`	Reverse-search command history. Start typing to filter.
`command1 | command2`	Pipe: feed output of one command into another.
`command > file.txt`	Redirect output to a file (overwrite).
`command >> file.txt`	Append output to a file.
`command 2>&1`	Redirect stderr to stdout.
`alias ll='ls -la'`	Create a shortcut. Add to ~/.bashrc to persist.
`screen -S mysession`	Start a named terminal session (survives disconnect).
`screen -r mysession`	Reattach to it.
`tmux`	More modern alternative to screen.

Tip: Add your favourite aliases to ~/.bashrc or ~/.zshrc (Kali uses zsh by default).

10 – Hackberry Pi CM5 – Hardware Tips

`vcgencmd measure_temp`	CPU temperature.
`vcgencmd get_throttled`	Check for thermal throttling (0x0 = all good).
`lsblk`	Confirm your boot device (SD vs NVMe).
`sudo fdisk -l /dev/nvme0n1`	Inspect NVMe SSD if installed.
`bluetoothctl`	Manage Bluetooth (for the onboard speakers).
`i2cdetect -y 1`	Scan I2C bus – see battery monitor, RTC, Stemma QT devices.
`sudo hwclock -r`	Read the RTC (CR927 battery backed).
`sudo hwclock -w`	Write system time to RTC.
`cat /sys/class/power_supply/*/voltage_now`	Read battery voltage (if exposed).

The keyboard is fully programmable via VIAL (vial.rocks). You can remap keys, create layers, and set up macros – worth doing to make the BlackBerry layout work for terminal use.

11 – Beginner Practice Projects

Project 1 – Map Your Home Network

Run nmap -sn against your home subnet to find every device. Then do a deeper scan (-sV) on each host. Document what you find: open ports, services, OS guesses. You'll be surprised what's running.

Project 2 – Set Up SSH & Go Headless

Enable SSH (systemctl enable --now ssh), find your Hackberry's IP, and SSH into it from your laptop. Now you have a real keyboard and screen. Set up key-based auth and disable password login. This teaches you SSH, keys, and service management.

Project 3 – Hack a Vulnerable VM

Download a deliberately vulnerable image like DVWA (Damn Vulnerable Web App) or try TryHackMe / HackTheBox free tiers from your Hackberry. Start with the guided beginner paths.

Project 4 – Write a Bash Script

Write a script that takes a subnet as an argument, runs a ping sweep, then does a service scan on any live hosts, and saves the output to a timestamped file. This teaches you scripting, piping, and automation.

Project 5 – Monitor Your Airspace

If you have an RTL-SDR dongle, plug it into one of the USB 3.0 ports and run dump1090 to receive ADS-B aircraft signals. The Hackberry makes a great portable receiver.

12 – Resources

OverTheWire Bandit (overthewire.org/wargames/bandit) – The best free interactive Linux command line tutorial. Start here.

TryHackMe (tryhackme.com) – Guided beginner-to-advanced security labs.

HackTheBox (hackthebox.com) – Capture-the-flag challenges.

Kali Docs (kali.org/docs) – Official documentation.

Hackberry GitHub (github.com/ZitaoTech/HackberryPiCM5) – Hardware docs, assembly guides, OS images.

explainshell.com – Paste any command and it breaks down every flag.

> **Use these tools ethically and legally. Only test systems you own or have explicit written authorization to test. Unauthorized access is a federal crime (CFAA in the US).**