Kali Linux Tools Guide

Top 50 pentesting tools shipped with Kali — what each one does, when to reach for it, and the single command that gets you started. For authorised testing only.

Reconnaissance

`nmap -sV -A target`	Service version + OS detection scan
`masscan -p1-65535 10.0.0.0/8 --rate=10000`	Internet-scale port scanner
`amass enum -d example.com`	Subdomain enumeration via OSINT sources
`subfinder -d example.com`	Fast passive subdomain discovery
`theharvester -d target.com -b all`	Emails, hosts, employees from public sources
`whatweb url`	Identify web tech stack
`wafw00f url`	Detect web application firewall
`whois domain.com`	Domain registration info
`dnsrecon -d target.com`	DNS enumeration suite
`recon-ng`	Modular OSINT framework
`shodan host 1.2.3.4`	Lookup internet-facing services

Web Application Testing

`burpsuite`	Intercepting proxy + scanner (industry standard)
`zaproxy`	OWASP ZAP — open-source Burp alternative
`sqlmap -u "url?id=1" --batch`	Automated SQL injection
`nikto -h url`	Web server vulnerability scanner
`dirb url /usr/share/wordlists/dirb/common.txt`	Directory brute-forcer
`gobuster dir -u url -w wordlist.txt`	Faster modern alternative
`ffuf -w list -u url/FUZZ`	Fast web fuzzer
`wpscan --url url`	WordPress vulnerability scanner
`xsser -u "url?q=XSS"`	XSS exploitation framework
`commix --url=url`	Command injection exploitation

Password Attacks

`hydra -L users -P passes ssh://target`	Network protocol bruteforce
`john --wordlist=rockyou.txt hash.txt`	CPU password cracker
`hashcat -m 0 -a 0 hash.txt rockyou.txt`	GPU password cracker (very fast)
`hashid hash`	Identify hash algorithm

`crunch 8 8 abc123 -o list.txt`	Generate custom wordlists
`cewl url -w wordlist.txt`	Build wordlist by spidering site
`medusa -u user -P passes -h host -M ssh`	Parallel login bruteforce
`cupp`	Common User Passwords Profiler

Wireless

`airmon-ng start wlan0`	Enable monitor mode
`airodump-ng wlan0mon`	Scan all nearby APs and clients
`aireplay-ng --deauth 10 -a BSSID wlan0mon`	Deauth attack to capture handshake
`aircrack-ng -w list.txt cap.cap`	Crack captured WPA2 handshake
`wifite`	Automated wireless audit (wraps the above)
`reaver -i wlan0mon -b BSSID`	WPS PIN attack
`kismet`	Passive wireless monitor and IDS

Exploitation Frameworks

`msfconsole`	Metasploit Framework console
`searchsploit keyword`	Search Exploit-DB locally
`msfvenom -p windows/meterpreter/reverse_tcp ...`	Generate payload
`beef-xss`	Browser Exploitation Framework
`setoolkit`	Social Engineering Toolkit
`exploit-db`	Browse/search public exploits

Post-Exploitation & Privilege Escalation

`linpeas.sh`	Linux privesc enumeration script
`winpeas.exe`	Windows equivalent
`linenum.sh`	Classic Linux enumeration
`pspy`	Watch processes without root (cron leak finder)
`mimikatz`	Windows credential dumper
`bloodhound`	AD attack path mapping
`crackmapexec smb hosts -u u -p p`	AD swiss army knife
`impacket-secretsdump u:p@host`	Extract domain hashes

Network & Sniffing

`wireshark`	GUI packet analyzer (the standard)
`tcpdump -i any -w out.pcap`	Headless capture
`tshark -r in.pcap -Y "http"`	CLI Wireshark filtering
`ettercap -G`	MITM toolkit (GUI)
`bettercap`	Modern MITM framework
`responder -I eth0`	LLMNR/NBT-NS poisoner — credential harvest
`arpspoof -i eth0 -t victim gw`	ARP cache poisoning

Forensics & Reverse Engineering

`autopsy`	Disk forensics GUI
`volatility -f mem.raw imageinfo`	Memory forensics
`binwalk -e file.bin`	Firmware extraction
`foremost -i image.dd`	File carving from raw images
`exiftool image.jpg`	Read all EXIF metadata
`ghidra`	NSA-released reverse engineering suite
`radare2 binary`	CLI reverse engineering framework
`strings -n 8 binary`	Find printable strings

Workflow Tips

- Always work in a VM with a snapshot. Reset between engagements.
- Document every command in a notes app — Cherrytree, Obsidian, or just a markdown file.
- Get written authorisation before scanning anything you do not own. Unauthorised scanning is illegal in most jurisdictions.
- Update tools weekly: `apt update && apt -y full-upgrade`.
- Practice on legal targets: TryHackMe, HackTheBox, OverTheWire, PortSwigger Web Academy.