KALI LINUX TOP 50 TOOLS 2026

Essential pentesting toolkit reference | sudoflare.com | Use only on systems you own or have permission to test

RECONNAISSANCE		
nmap	Network scanner	`nmap -sV -O target`
theHarvester	Email/subdomain OSINT	`theHarvester -d domain.com -b google`
shodan	IoT/device search	`shodan search 'apache 2.4'`
maltego	Link analysis GUI	`maltego`
recon-ng	Web recon framework	`recon-ng`
dnsrecon	DNS enumeration	`dnsrecon -d domain.com`
dnsenum	DNS brute force	`dnsenum domain.com`
fierce	DNS/subnet scanner	`fierce --domain domain.com`
WEB APP TESTING		
burpsuite	Web proxy & scanner	`burpsuite`
nikto	Web server scanner	`nikto -h http://target`
gobuster	Dir/file brute force	`gobuster dir -u http://t -w wordlist`
sqlmap	SQL injection auto	`sqlmap -u 'http://t/?id=1'`
wfuzz	Web fuzzer	`wfuzz -c -w wordlist http://t/FUZZ`
ffuf	Fast web fuzzer	`ffuf -u http://t/FUZZ -w list`
wpscan	WordPress scanner	`wpscan --url http://wp-site`
xsser	XSS testing tool	`xsser --url http://t/page`
EXPLOITATION		
metasploit	Exploit framework	`msfconsole`
searchsploit	Exploit DB search	`searchsploit apache 2.4`
msfvenom	Payload generator	`msfvenom -p windows/shell -f exe`
beef	Browser exploit FW	`beef-xss`
social-engineer	SE toolkit	`setoolkit`
routersploit	Router exploits	`rsf`

exploitdb	Exploit database	`searchsploit -m 12345`
PASSWORD ATTACKS		
hashcat	GPU password crack	`hashcat -m 0 hash.txt wordlist`
john	Password cracker	`john --wordlist=rockyou hash`
hydra	Network brute force	`hydra -l user -P list ssh://t`
medusa	Parallel brute force	`medusa -h t -u user -P list -M ssh`
crunch	Wordlist generator	`crunch 8 8 -t @@###%%%`
cewl	Website wordlist gen	`cewl http://target -w words.txt`
hash-identifier	ID hash type	`hash-identifier`
WIRELESS		
aircrack-ng	WiFi auditing suite	`aircrack-ng -w wordlist cap`
airmon-ng	Enable monitor mode	`airmon-ng start wlan0`
airodump-ng	WiFi packet capture	`airodump-ng wlan0mon`
aireplay-ng	WiFi packet inject	`aireplay-ng -0 5 -a BSSID`
wifite	Automated WiFi attack	`wifite`
kismet	Wireless detector	`kismet`
fern-wifi-cracker	WiFi GUI cracker	`fern-wifi-cracker`
POST-EXPLOIT & FORENSICS		
mimikatz	Windows cred dump	`(windows) mimikatz.exe`
linpeas	Linux priv-esc enum	`./linpeas.sh`
winpeas	Windows priv-esc	`winpeas.exe`
volatility	Memory forensics	`vol.py -f mem.dmp`
autopsy	Digital forensics	`autopsy`
binwalk	Firmware analysis	`binwalk firmware.bin`
wireshark	Network analysis	`wireshark`
tcpdump	CLI packet capture	`tcpdump -i eth0 -w cap.pcap`