Kali Linux – 100 Essential Commands & Tools

Professional Cheat Sheet for Ethical Hacking & Cyber Security

1. **nmap** – Network scanning and service discovery tool
2. **nikto** – Web server vulnerability scanner
3. **sqlmap** – Automated SQL injection testing tool
4. **hydra** – Fast login brute force attack tool
5. **airmon-ng** – Enable monitor mode on wireless interfaces
6. **airodump-ng** – Capture wireless packets
7. **aireplay-ng** – Inject packets into wireless network
8. **aircrack-ng** – Crack WEP/WPA Wi-Fi passwords
9. **reaver** – Brute force WPS PIN to recover WPA key
10. **wash** – Detect WPS enabled access points
11. **metasploit** – Framework for penetration testing
12. **msfconsole** – Launch Metasploit interactive console
13. **searchsploit** – Search exploit database
14. **john** – Password cracking tool
15. **hashcat** – Advanced password recovery tool
16. **wpscan** – WordPress vulnerability scanner
17. **dirb** – Web content directory scanner
18. **dirsearch** – Advanced directory brute forcing tool
19. **gobuster** – Directory and DNS brute force tool
20. **whatweb** – Identify website technologies
21. **theHarvester** – Gather emails and subdomains
22. **whois** – Get domain registration information
23. **dnsenum** – DNS enumeration tool
24. **dnsrecon** – Advanced DNS reconnaissance
25. **netcat** – Read/write data across networks
26. **nc** – Short form of netcat
27. **tcpdump** – Capture and analyze network packets
28. **wireshark** – GUI-based network protocol analyzer
29. **ettercap** – Man-in-the-middle attack tool
30. **bettercap** – Modern MITM attack framework
31. **hping3** – Packet crafting and firewall testing
32. **masscan** – High-speed network port scanner
33. **snmpwalk** – SNMP enumeration tool
34. **snmpcheck** – SNMP security audit

35. **enum4linux** – SMB enumeration tool
36. **smbclient** – Access SMB/CIFS shares
37. **crackmapexec** – Post-exploitation tool
38. **impacket** – Network protocol exploitation toolkit
39. **responder** – LLMNR, NBT-NS poisoning tool
40. **evil-winrm** – WinRM shell for Windows targets
41. **ftp** – File transfer protocol client
42. **ssh** – Secure shell remote login
43. **scp** – Secure file copy over SSH
44. **rsync** – Remote file synchronization
45. **curl** – Transfer data from URLs
46. **wget** – Download files from web
47. **openssl** – SSL/TLS cryptography tool
48. **sslscan** – Scan SSL/TLS vulnerabilities
49. **sslyze** – Analyze SSL configuration
50. **burpsuite** – Web application security testing
51. **zap** – OWASP ZAP web scanner
52. **feroxbuster** – Fast content discovery tool
53. **amass** – Subdomain enumeration
54. **sublist3r** – Subdomain discovery tool
55. **xfreerdp** – Remote desktop client
56. **rdesktop** – RDP client for Linux
57. **arp-scan** – Discover devices on local network
58. **netdiscover** – ARP reconnaissance tool
59. **macchanger** – Change MAC address
60. **iptables** – Firewall configuration tool
61. **ufw** – Uncomplicated firewall
62. **chkrootkit** – Rootkit detection tool
63. **lynis** – System security audit tool
64. **clamav** – Antivirus scanner
65. **msfvenom** – Payload generator
66. **payloadsallthethings** – Payload reference collection
67. **crunch** – Wordlist generator
68. **cewl** – Custom wordlist generator
69. **fcrackzip** – ZIP password cracking
70. **pdfcrack** – PDF password cracking
71. **binwalk** – Firmware analysis tool
72. **strings** – Extract readable strings from files

73. **file** – Detect file type
74. **exiftool** – Read file metadata
75. **volatility** – Memory forensics framework
76. **autopsy** – Digital forensics platform
77. **foremost** – Recover deleted files
78. **setoolkit** – Social engineering toolkit
79. **beef-xss** – Browser exploitation framework
80. **proxychains** – Route traffic through proxy
81. **tor** – Anonymous communication network
82. **anonsurf** – Route system traffic through Tor
83. **tmux** – Terminal multiplexer
84. **screen** – Terminal session manager
85. **htop** – Interactive process viewer