LINUX.SECURE.SCALABLE
Master Linux, Master Cybersecurity Power!

Top 150 Kali Linux Commands Every Cybersecurity Enthusiast Must Know!

RAHUL KAPATE
www.cybersecurityrahul.in

1. Basic Linux Commands

---

1. ls - List directory contents
2. cd - Change directory
3. pwd - Print working directory
4. mkdir - Create a new directory
5. rmdir - Remove empty directories
6. rm - Remove files or directories
7. cp - Copy files and directories
8. mv - Move or rename files
9. touch - Create an empty file
10. find - Search for files
11. locate - Find files by name
12. updatedb - Update locate database
13. cat - View file contents
14. less - View file contents page by page
15. nano - Open a text editor

16. vi - Open the Vi text editor
17. echo - Display text in terminal
18. history - Show command history
19. clear - Clear terminal screen
20. whoami - Show the current user
21. id - Show user ID and group ID
22. chmod - Change file permissions
23. chown - Change file owner
24. stat - Show file metadata
25. df - Show disk space usage
26. du - Show directory size
27. mount - Mount a file system
28. umount - Unmount a file system
29. tar - Compress/extract .tar files
30. zip - Compress files into .zip
31. unzip - Extract .zip files
32. wget - Download files from the web
33. curl - Fetch data from URLs
34. ping - Test network connectivity
35. traceroute - Trace network hops
36. arp - Show ARP table
37. ifconfig - Show network interface details (deprecated)
38. ip a - Show IP addresses

39. ip route - Show routing table
40. netstat - Show network connections (deprecated)
41. ss - Show active connections
42. nslookup - Query DNS
43. dig - Perform advanced DNS queries
44. whois - Look up domain details
45. uptime - Show system uptime
46. free - Show memory usage
47. top - Show running processes
48. htop - Interactive process viewer
49. kill - Terminate a process
50. pkill - Kill processes by name
51. ps - Show running processes
52. bg - Resume a job in the background
53. fg - Resume a job in the foreground
54. nohup - Run a command immune to hangups
55. alias - Create a shortcut for a command
56. unalias - Remove an alias
57. uname - Show system information
58. lsb_release -a - Show OS details
59. shutdown - Shutdown the system
60. reboot - Restart the system

2. User & Group Management

61. adduser - Add a new user
62. userdel - Delete a user
63. passwd - Change user password
64. groupadd - Create a new group
65. groupdel - Delete a group
66. usermod - Modify a user
67. groups - Show user’s groups
68. su - Switch user
69. sudo - Run a command as root
70. visudo - Edit sudoers file
71. chage - Manage password expiry
72. last - Show login history
73. w - Show logged-in users
74. who - Show who is logged in
75. finger - Show user information

3. File Permissions & Ownership

76. ls -l - Show file permissions
77. chmod 777 file - Give full permissions
78. chmod 755 file - Give execute permissions
79. chown user:group file - Change ownership

80. umask - Set default permissions

81. getfacl - Get ACL details

82. setfacl - Modify ACL settings

4. Package Management (APT)

---

83. apt update - Refresh repositories

84. apt upgrade - Upgrade installed packages

85. apt install package - Install a package

86. apt remove package - Remove a package

87. apt autoremove - Remove unused packages

88. apt list --installed - Show installed packages

89. dpkg -i package.deb - Install a .deb package

90. dpkg -r package - Remove a .deb package

91. dpkg -l - List installed .deb packages

5. Network Scanning & Security

---

92. nmap - Scan networks and hosts

93. nmap -sP 192.168.1.0/24 - Ping sweep

94. nmap -sV - Service version detection

95. nmap -A - Aggressive scan

96. nmap -O - Detect OS

97. tcpdump - Capture network packets

98. wireshark - GUI network analyzer

99. tshark - CLI packet capture

100. netcat - Listen on a port

101. nc -zv target 80 - Check open ports

102. aircrack-ng - Crack Wi-Fi passwords

103. airmon-ng - Enable monitor mode

104. airoscript-ng - Automate Wi-Fi attacks

105. macchanger - Change MAC address

6. Password Cracking

---

106. hydra - Brute force login

107. john - John the Ripper password cracker

108. hashcat - Advanced password recovery

109. cupp - Custom wordlist generator

110. crunch - Wordlist generator

7. Web Penetration Testing

---

111. sqlmap - Automated SQL injection

112. wpscan - WordPress security scanner

113. gobuster - Directory brute-forcing

114. dirb - Directory search

115. sublist3r - Subdomain enumeration

116. nikto - Web vulnerability scanner

117. burpsuite - Web security tool

8. Exploitation & Payloads

---

118. metasploit - Penetration testing framework

119. msfconsole - Open Metasploit

120. msfvenom - Create payloads

121. exploitdb - Search exploits

122. armitage - GUI for Metasploit

9. Post Exploitation

---

123. mimikatz - Extract Windows credentials

124. empire - PowerShell post-exploitation

125. beef - Browser Exploitation Framework

126. responder - Network credential harvesting

10. Forensics & Reverse Engineering

127. volatility - Memory forensics
128. binwalk - Firmware analysis
129. foremost - File recovery
130. autopsy - Digital forensic analysis
131. strings - Extract strings from binaries
132. ghidra - Reverse engineering tool
133. gdb - GNU Debugger

11. Wireless Attacks

134. reaver - WPS attack tool
135. fern-wifi-cracker - GUI for Wi-Fi hacking
136. kismet - Wireless network detector

12. Miscellaneous

137. ssh - Connect to a remote system

138. scp - Securely copy files

139. rsync - Sync directories

140. cron - Schedule tasks

141. at - Schedule one-time tasks

142. strace - Trace system calls

143. lsof - List open files