Cybersecurity Terminal & Tools Guide (2-Page PDF)

■ BASIC TERMINAL COMMANDS (Linux)

- pwd: Show current directory
- ls / ls -l: List files and folders (detailed with -l)
- cd folder / cd ..: Move into or out of folders
- mkdir folder: Create folder
- touch file.txt: Create empty file
- rm file.txt / rm -r folder: Delete file or folder with contents
- cp a b / mv a b: Copy or move files
- cat file.txt / nano file.txt: Show or edit file
- clear: Clear screen

■■ INTERMEDIATE / ADVANCED COMMANDS

- chmod 755 file: Change file permissions
- chown user:group file: Change file owner
- find / -name file.txt: Search for file by name
- grep 'word' file.txt: Search inside file for word
- history / head / tail: Command history, view file lines
- ps aux / top / htop: View running processes
- kill PID: Kill process by ID
- netstat -tuln: View open network ports
- curl ifconfig.me: Show public IP
- sudo command: Run as admin
- tar -xvzf file.tar.gz: Extract compressed file

Top 10 Cybersecurity Tools to Learn

■■ TOP CYBERSECURITY TOOLS

1. Nmap – Network Scanner
- Scans live hosts, ports, services. Ex: nmap -sV 192.168.1.1

2. Wireshark – Packet Analyzer
- Captures and inspects network traffic in real-time

3. Burp Suite – Web Security Testing
- Intercepts, modifies, replays HTTP requests. Great for bug bounty.

4. Nikto – Web Server Scanner
- Scans web servers for known vulnerabilities. Ex: nikto -h http://site.com

5. Metasploit – Exploitation Framework
- Launches payloads/exploits to test vulnerabilities

6. John the Ripper – Password Cracker
- Cracks password hashes (SHA, MD5, etc.)

7. Hydra – Brute Force Tool
- Brute forces login forms. Ex: hydra -l user -P wordlist.txt ssh://ip

8. sqlmap – SQL Injection Tool
- Auto-tests and exploits SQLi. Ex: sqlmap -u http://site.com/page?id=1 --dbs

9. Aircrack-ng – Wireless Cracker
- Captures & cracks WPA/WEP Wi-Fi passwords

10. Autopsy – Digital Forensics GUI
- Recover deleted files, analyze system history, disk images

■ Practice Platforms: TryHackMe, HackTheBox, OverTheWire, VulnHub

■■■ Use Kali Linux or Parrot OS to try these tools safely