Cyber Warfare Training Guide

1. Setting up a Legal Hacking Lab (Kali, Metasploitable, DVWA)
2. Scanning networks with Nmap and Masscan
3. Exploiting known vulnerabilities using Metasploit
4. Brute-force login forms with Hydra & BurpSuite
5. Packet sniffing with Wireshark (HTTP, DNS, FTP analysis)
6. Wireless hacking simulation with Wifite & Aircrack-ng
7. Phishing simulations with SET (Social Engineering Toolkit)
8. Creating custom payloads with msfvenom
9. Reverse shells and Netcat practices
10. Password cracking using John the Ripper & Hashcat
11. Log file analysis and basic forensics
12. Setting up anonymous browsing with TOR and ProxyChains
13. OSINT techniques to gather intel on targets
14. Exploit research and CVE-based attack labs
15. DNS spoofing and MITM simulation
16. WiFi Evil Twin attacks for training
17. Linux privilege escalation paths
18. Web Application hacking with OWASP Top 10
19. Malware analysis (Basic static & dynamic)
20. Creating a red team scenario & reporting