3-Month Cybersecurity Curriculum (Ethical Hacking Focus)

This curriculum is designed for a 3-month intensive training program focused on Ethical Hacking. It follows a project-based approach with 3 sessions per week (2–3 hours per session). The tools used include Kali Linux, Metasploit, Nmap, Burp Suite, and TryHackMe labs. The goal is to develop practical penetration testing skills and a strong cybersecurity foundation.

Month 1: Foundations of Ethical Hacking

Focus: Cybersecurity basics, Linux proficiency, networking, reconnaissance, and scanning.

Weekly Breakdown

Week 1: Introduction & Environment Setup
- Setting up Kali Linux (VMware/VirtualBox)
- Linux essentials for hackers
- Introduction to cybersecurity & ethical hacking principles
- Project: Set up a secure lab environment

Week 2: Networking & Protocols
- TCP/IP, DNS, HTTP/HTTPS, ARP
- Packet analysis using Wireshark
- Project: Capture and analyze packets from local traffic

Week 3: Reconnaissance & Scanning
- Passive reconnaissance (WHOIS, nslookup, Google dorking)
- Active reconnaissance with Nmap
- Vulnerability scanning basics
- Project: Perform reconnaissance and port scan on a target VM

Week 4: Web Basics & Burp Suite
- HTTP requests/responses
- Burp Suite setup and usage
- Project: Analyze and intercept HTTP traffic using Burp Suite

Month 2: Exploitation & Attacks

Focus: Vulnerability exploitation, Metasploit, web attacks, privilege escalation.

Weekly Breakdown

Week 5: Vulnerability Assessment
- Common vulnerabilities (OWASP Top 10)
- Using OpenVAS/Nessus (if available)
- Project: Scan a target VM for vulnerabilities

Week 6: Exploitation with Metasploit
- Metasploit basics
- Exploiting common services (FTP, SMB, HTTP)
- Project: Exploit a vulnerable machine on TryHackMe

Week 7: Web Application Hacking
- SQL Injection, XSS, CSRF basics
- Burp Suite intruder & repeater
- Project: Exploit vulnerabilities in a web app lab

Week 8: Privilege Escalation & Persistence
- Linux/Windows privilege escalation techniques
- Maintaining access with backdoors
- Project: Escalate privileges on a CTF-style machine

Month 3: Advanced Topics & Final Project

Focus: Wireless, post-exploitation, real-world simulation, and reporting.

Weekly Breakdown

Week 9: Wireless & Password Attacks
- Cracking WiFi with Aircrack-ng
- Brute-force and dictionary attacks (Hydra, John the Ripper)
- Project: Crack a WPA2 handshake in lab

Week 10: Post-Exploitation & Lateral Movement
- Extracting credentials, pivoting
- Persistence techniques
- Project: Simulate lateral movement in a small lab network

Week 11: Capture the Flag (CTF) Practice
- Solve real-world hacking challenges on TryHackMe/HackTheBox
- Project: Complete 2–3 guided CTF challenges

Week 12: Final Project & Reporting
- Full penetration test simulation
- Writing a professional penetration testing report
- Project: Perform an end-to-end penetration test on a target VM and present findings