Cybersecurity Professional Program

Cybersecurity Professional Program

3-Month Integrated Training Outline

Month 1: Security Governance, Networking & Reconnaissance

Goal: Build a theoretical foundation in security principles while mastering the art of information gathering.

Week 1: Foundations of Security & Networking

- **Security Principles:** The CIA Triad, (ISC)² Code of Ethics, and Ethical Hacking legal implications.
- **Networking:** Deep dive into OSI vs. TCP/IP models, IP addressing (IPv4/IPv6), and essential protocols (TCP/UDP, ICMP).
- **Network Infrastructure:** Understanding the roles of Switches, Routers, and Firewalls in a secure architecture.

Week 2: Security Principles & Lab Setup

- **Access Management:** Authentication (MFA), Authorization, and the Principle of Least Privilege.
- **Virtualization:** Setting up VMware/VirtualBox with Kali Linux and vulnerable targets (Metasploitable).
- **Linux Mastery:** Filesystem hierarchy, user management, and essential CLI commands for security auditing.

Week 3: Risk Management, BC/DR & Footprinting

- **Strategy:** Risk treatment (Avoid, Transfer, Mitigate, Accept) and Business Continuity/Disaster Recovery planning.
- **Reconnaissance:** Passive footprinting using Google Dorks, Whois, and Social Media OSINT.
- **Scanning:** Active host discovery and port/service identification using Nmap.

Week 4: Vulnerability Assessment (VA) & Incident Response

- **Methodology:** Understanding CVE/CVSS scores and the Incident Response Lifecycle (Detection to Recovery).
- **Tooling:** Running automated scans with Nessus and Acunetix to identify system flaws.
- **Project 1:** Conduct a Risk Assessment for a mock business and draft a formal Security Policy.

Month 2: Network Defense & Web Exploitation

Goal: Master the technical aspects of securing network traffic and exploiting web-based vulnerabilities.

Week 5: Access Control & Directory Enumeration

- **Models:** Mandatory (MAC), Discretionary (DAC), and Role-Based Access Control (RBAC).
- **Enumeration:** Discovering hidden web directories using Gobuster, FFuf, and Dirsearch.
- **Brute Force:** Executing credential attacks using Hydra and creating effective wordlists.

Week 6: Network Security Fundamentals & Burp Suite

- **Defense:** Securing layers 1-7 of the OSI model and configuring secure protocols (HTTPS, SSH, SFTP).
- **Web Proxy:** Configuring Burp Suite for request interception, modification, and analysis.
- **Metasploit:** Introduction to the framework—Exploits, Payloads, and Auxiliaries.

Week 7: Advanced Network Defense & SQL Injection

- **Segmentation:** Utilizing VLANs and DMZs; introduction to IDS/IPS (Snort).
- **SQLi:** Manual and automated SQL Injection techniques to manipulate backend databases.
- **DDoS:** Understanding Denial of Service attack vectors and mitigation strategies.

Week 8: Web Pentesting (XSS, LFI, SSRF)

- **Client-Side:** Reflected and Stored Cross-Site Scripting (XSS).
- **Server-Side:** Local File Inclusion (LFI) to RCE, SSRF, and CSRF exploitation.

Project 2: Design a secure, segmented network architecture with specific firewall rules to block unauthorized traffic.

Month 3: Security Operations & Advanced Specialized Domains

Goal: Transition into enterprise-level security operations and finalize certification readiness.

Week 9: SecOps, Windows & Active Directory (AD)

- **Operations:** Data classification, Patch Management, and System Hardening for Windows/Linux.
- **AD Security:** Domain Controller setup, Active Directory configuration, and Group Policy implementation.
- **Hardening:** Network Access Control (NAC) and Privilege Access Management (PAM).

Week 10: Cloud Security, Social Engineering & APIs

- **Cloud:** Understanding IaaS, PaaS, SaaS, and the Shared Responsibility Model.
- **Social Engineering:** Phishing vectors, human-based attacks, and Security Awareness.
- **API Security:** Identifying vulnerabilities in REST APIs using Postman.

Week 11: Cryptography, Malware & CC Review

- **Crypto:** Symmetric/Asymmetric encryption, Hashing, and Public Key Infrastructure (PKI).
- **Malware:** Analysis of virus lifecycles, Ransomware, and anti-evasion basics.
- **CC Prep:** Comprehensive domain review and timed mock exams for the (ISC)² CC certification.

Week 12: Final Capstone & Career Readiness

- **Capstone Project:** Perform a full-scale security audit and "Live Hacking" of an enterprise lab environment, delivering a remediation roadmap.
- **SOC/SIEM:** Practical log analysis and an overview of SIEM tool architecture.
- **Career:** Technical resume building, LinkedIn optimization, and mock interview simulations.