TRAINING PROGRAM

Cyber Security Engineering Course

Beginner to Security Engineer

A comprehensive 8-week journey to master ethical hacking, network defense, and build production-ready secure systems.

DURATION	LEVEL	FORMAT
8 Weeks	**Professional**	**Hands-on Lab**

Table of Contents

1 Course Objective

Transform Learners into Security Engineers

This comprehensive course is designed to take beginners and transform them into capable Security Engineers who can:

- Identify and mitigate vulnerabilities in systems and applications.
- Perform professional-grade penetration testing using industry tools.
- Secure corporate networks and cloud infrastructures.
- Implement robust encryption and authentication mechanisms.

2 Program Structure

Attribute	Details
Duration	8 Weeks (2 Months)
Weekly Schedule	2 Days Learning + 2 Days Practice + 1 Day Demo
Total Phases	6 Progressive Phases
Final Deliverable	Capstone Security Audit / Project

The program follows a consistent weekly pattern: **Monday-Tuesday** for learning new concepts, **Wednesday-Thursday** for hands-on practice, and **Friday** for demos.

3 Phase 1: Security Fundamentals

Duration: Week 1

- Cyber Security Landscape: Malware, Phishing, Ransomware.
- The CIA Triad: Confidentiality, Integrity, and Availability.
- Ethics & Legal: Cyber Laws, HIPAA, GDPR.
- Introduction to Linux for Security: Kernel and Permissions.

- **OS:** Kali Linux / Parrot Security OS.
- **Virtualization:** VirtualBox or VMware.

- **Secure Lab Setup:** Create an isolated virtualized sandbox.
- **Linux Hardening:** Audit user permissions and scripts.

Learning Outcome: Students will establish a strong security foundation.

4 Phase 2: Network Security

Duration: Week 2

- OSI/TCP-IP models from a security perspective.
- Protocols: DNS, SSH, HTTP/S, and TLS/SSL.
- Firewalls, IDS, and IPS fundamentals.

- **Packet Analysis:** Use Wireshark to detect cleartext credentials.
- **Network Mapper:** Identify active services using Nmap.

5 Phase 3: System Hardening

Duration: Week 3

- OS Security: Windows vs. Linux hardening.
- Password Attacks: Hashing and Brute-forcing.
- Privilege Escalation: SUID and SUDO misconfigurations.

- **Hash Cracker:** Use John the Ripper to recover passwords.
- **Permission Auditor:** Identify Linux vulnerabilities.

6 Phase 4: Ethical Hacking & Recon

Duration: Week 4

- OSINT: Open Source Intelligence gathering.
- Active vs. Passive Reconnaissance.
- Vulnerability Scanning with Nessus.

- **Company Profile:** Perform a full OSINT report.
- **Vulnerability Scan:** Run an audit on a legacy VM.

7 Phase 5: Web Application Security

Duration: Week 5-6

- **OWASP Top 10:** SQL Injection, XSS, CSRF, and IDOR.
- Intercepting Proxies: Burp Suite Proxy usage.
- Cryptography: AES and RSA encryption models.

- **Proxy:** Burp Suite.
- **Vulnerable Apps:** OWASP Juice Shop.

- **SQLi Lab:** Bypass login screens via injection.
- **XSS Hunter:** Execute scripts to capture session cookies.

8 Phase 6: Cloud & Advanced Defense

Duration: Week 7

- Cloud Security: AWS S3 misconfigurations.
- MITM Attacks: ARP Spoofing and DNS Poisoning.
- Incident Response foundations.

9 Final Project

Duration: Week 8

1. **Web App Pentest Report:** Conduct a full audit and write a report.
2. **Secure Network Design:** Build a network with VLANs and Firewalls.
3. **CTF Challenge:** Complete a custom ”Capture The Flag” environment.

10 Recommended Technology Stack

Category	Preferred Tools
Offensive OS	Kali Linux, Parrot Security OS
Networking	Wireshark, Nmap, Netcat
Web Audit	Burp Suite, OWASP ZAP
Exploitation	Metasploit, Sqlmap
Cryptography	GPG, OpenSSL, Hashcat

11 Weekly Execution Plan

Day	Activity	Focus
Monday	Learning	Theory & Models
Tuesday	Learning	Tool Mechanics
Wednesday	Practice	Guided Lab
Thursday	Build	Independent Work
Friday	Demo	Presentation

12 Evaluation Metrics

Metric	Description	Weight
Lab Reports	Accuracy of exploit docs	30%
Recon Quality	Thoroughness of recon	20%
Project Report	Professionalism of VAR	40%
CTF Score	Success in challenges	10%

13 Learning Outcomes

- **Professional Auditing:** Perform tests following industry standards.
- **Web Defense:** Remediate OWASP Top 10 vulnerabilities.
- **Network Analysis:** Detect malicious traffic patterns.
- **Reporting:** Write technical reports for executive audiences.

14 Career Path

This course leads to roles such as **Junior Penetration Tester, Security Analyst,** and **SOC Engineer**.

End of Syllabus — Cyber Security Engineering v1.1