Course Title: Ethical Hacking - Red Teaming
Duration: 4 Months (16 Weeks)
Mode: Hybrid Classes
Level: Intermediate
Labs and Projects: 18 Practical Labs and Projects
Language: English

Month 1: Foundations of Ethical Hacking

Module 1: Networking Refresher

- Introduction
- IP Addresses
- MAC Addresses
- TCP, UDP, and the Three-Way Handshake
- Common Ports and Protocols
- The OSI Model
- Subnetting Part 1 & 2
- Quiz: Networking Basics

Module 2: Lab Environment Setup

- Installing VMWare / VirtualBox
- Configuring VirtualBox
- Installing Kali Linux
- Setting Up Vulnerable Machines (e.g., Kioptrix)
- Project: Building a Hacking Lab

Month 2: Information Gathering and Scanning

Module 3: Ethical Hacking Methodology

- The Five Stages of Ethical Hacking
- Quiz: Hacking Fundamentals

Module 4: Information Gathering (Reconnaissance)

- Passive Reconnaissance Overview
- Identifying Targets, Email Addresses, and Credentials
- Hunting Subdomains and Website Technologies
- Information Gathering with Burp Suite
- Social Media OSINT
- Quiz: Information Gathering Techniques

Module 5: Scanning and Enumeration

- Scanning with Nmap
- Enumerating HTTP, HTTPS, SMB, SSH
- Researching Potential Vulnerabilities
- Project: Documenting Reconnaissance and Scanning Results

Month 3: Vulnerability Exploitation and Web App Attacks

Module 6: Vulnerability Scanning

- Scanning with Nessus
- Quiz: Vulnerability Scanning Techniques

Module 7: Exploitation Basics

- Reverse Shells vs. Bind Shells
- Staged vs. Non-Staged Payloads
- Gaining Root with Metasploit
- Manual Exploitation
- Brute Force Attacks, Credential Stuffing, and Password Spraying
- Quiz: Exploitation Techniques

Module 8: Web Application Attacks

- SQL Injection (Union, Blind)

- Cross-Site Scripting (XSS) - DOM, Stored
- Command Injection
- Insecure File Uploads - Bypass Techniques
- Attacking Authentication - Brute Force and MFA
- Project: Web App Exploitation Lab

Month 4: Advanced Topics and Reporting

Module 9: Active Directory Attacks

- Active Directory Fundamentals
- Attacking Initial Vectors (LLMNR Poisoning, SMB Relay)
- Post-Compromise Enumeration (ldapdomaindump, Bloodhound)
- Post-Compromise Attacks (Pass-the-Hash, Kerberoasting)
- Project: Active Directory Attack Simulation

Module 10: Post-Exploitation Techniques

- Maintaining Access and Pivoting
- Cleaning Up After Exploitation
- File Transfers and Lateral Movement
- Quiz: Post-Exploitation Strategies

Module 11: Web Application Enumeration and Exploitation Revisited

- Finding Subdomains with Assetfinder and Amass
- Automating Enumeration with Scripts
- SQL Injection and XSS Challenges
- Project: Capture the Flag (CTF) Challenge

Module 12: Reporting and Career Preparation

- Legal Documents and Reporting
- Pentest Report Writing

- Reviewing a Real Pentest Report
- Career Advice for Ethical Hackers
- Final Exam and Project Submission: Comprehensive Pentest Report

Capstone Project:

- Real-World Penetration Test Simulation
    - Conduct a complete penetration test on a simulated environment
    - Document findings, exploited vulnerabilities, and remediation steps
    - Submit a detailed penetration testing report