# Penetration Testing and Ethical Hacking: From Beginner to Expert

————————

### **Module 1: Introduction to Penetration Testing**

* **Lesson 1.1:** Understanding Cybersecurity Fundamentals
* **Lesson 1.2:** The Role of a Penetration Tester
* **Lesson 1.3:** Setting Up a Lab Environment
* [\*\*Lesson 1.4:\*\* Overview of Cyber Attack Vectors](bear://x-callback-url/open-note?title=%2A%2ALesson%201%2E4%3A%2A%2A%20Overview%20of%20Cyber%20Attack%20Vectors)
* [\*\*Lesson 1.5:\*\* Common Tools and Software Used in PenTesting](bear://x-callback-url/open-note?title=%2A%2ALesson%201%2E5%3A%2A%2A%20Common%20Tools%20and%20Software%20Used%20in%20PenTesting)

### **Module 2: Networking Basics**

* **Lesson 2.1:** Network Topologies and Protocols
* **Lesson 2.2:** The OSI and TCP/IP Models
* **Lesson 2.3:** Understanding IP Addressing and Subnetting
* **Lesson 2.4:** Introduction to DNS and DHCP
* **Lesson 2.5:** Network Devices and Their Functions

### **Module 3: Linux and Windows Fundamentals**

* **Lesson 3.1:** Basic Linux Commands and File System
* **Lesson 3.2:** Windows Command Line and PowerShell
* **Lesson 3.3:** User and Permission Management
* **Lesson 3.4:** Process and Service Management
* **Lesson 3.5:** Scripting Basics for Automation

### **Module 4: Reconnaissance and Information Gathering**

* **Lesson 4.1:** Passive Reconnaissance Techniques
* **Lesson 4.2:** Active Reconnaissance Methods
* **Lesson 4.3:** Utilizing Open Source Intelligence (OSINT)
* **Lesson 4.4:** Social Engineering Fundamentals
* **Lesson 4.5:** Identifying Targets and Entry Points

### **Module 5: Scanning and Enumeration**

* **Lesson 5.1:** Network Scanning with Nmap
* **Lesson 5.2:** Vulnerability Scanning Tools
* **Lesson 5.3:** Service and Version Detection
* **Lesson 5.4:** Banner Grabbing Techniques
* **Lesson 5.5:** Enumerating Users and Shares

### **Module 6: Vulnerability Analysis**

* **Lesson 6.1:** Understanding Common Vulnerabilities
* **Lesson 6.2:** Working with CVEs and Security Advisories
* **Lesson 6.3:** Automated Vulnerability Scanners
* **Lesson 6.4:** Manual Vulnerability Discovery
* **Lesson 6.5:** Prioritizing Vulnerabilities for Exploitation

### **Module 7: Exploitation Techniques**

* **Lesson 7.1:** Introduction to Exploitation
* **Lesson 7.2:** Exploiting Network Services
* **Lesson 7.3:** Client-Side Exploits
* **Lesson 7.4:** Web Application Exploitation
* **Lesson 7.5:** Privilege Escalation Methods

### **Module 8: Post-Exploitation Strategies**

* **Lesson 8.1:** Maintaining Access with Backdoors
* **Lesson 8.2:** Data Exfiltration Techniques
* **Lesson 8.3:** Lateral Movement within Networks
* **Lesson 8.4:** Clearing Logs and Covering Tracks
* **Lesson 8.5:** Advanced Persistent Threats (APTs)

### **Module 9: Web Application Penetration Testing**

* **Lesson 9.1:** Web Technologies Overview
* **Lesson 9.2:** The OWASP Top Ten Vulnerabilities
* **Lesson 9.3:** SQL Injection Attacks
* **Lesson 9.4:** Cross-Site Scripting (XSS)
* **Lesson 9.5:** Web Application Firewalls and Bypassing

### **Module 10: Wireless Network Attacks**

* **Lesson 10.1:** Wireless Networking Basics
* **Lesson 10.2:** Wireless Security Protocols
* **Lesson 10.3:** Cracking Wireless Encryption
* **Lesson 10.4:** Rogue Access Points and Evil Twins
* **Lesson 10.5:** Bluetooth and NFC Attacks

### **Module 11: Mobile Device and Application Security**

* **Lesson 11.1:** Mobile Operating Systems Overview
* **Lesson 11.2:** Mobile Application Vulnerabilities
* **Lesson 11.3:** Mobile Device Management (MDM) Exploits
* **Lesson 11.4:** Reverse Engineering Mobile Apps
* **Lesson 11.5:** Secure Mobile Development Practices

### **Module 12: Advanced Exploitation Techniques**

* **Lesson 12.1:** Buffer Overflow Exploitation
* **Lesson 12.2:** Format String Attacks
* **Lesson 12.3:** Return-Oriented Programming (ROP)
* **Lesson 12.4:** Exploit Development with Metasploit
* **Lesson 12.5:** Bypassing Security Mechanisms (ASLR, DEP)

### **Module 13: Malware and Reverse Engineering**

* **Lesson 13.1:** Types of Malware and Their Behaviors
* **Lesson 13.2:** Static and Dynamic Analysis Techniques
* **Lesson 13.3:** Disassemblers and Debuggers
* **Lesson 13.4:** Obfuscation and Anti-Analysis Techniques
* **Lesson 13.5:** Writing Custom Shellcode

### **Module 14: Cloud Security and Penetration Testing**

* **Lesson 14.1:** Cloud Computing Models and Services
* **Lesson 14.2:** Security Challenges in Cloud Environments
* **Lesson 14.3:** Attacking Cloud Infrastructure
* **Lesson 14.4:** Container Security (Docker, Kubernetes)
* **Lesson 14.5:** Protecting Cloud Assets

### **Module 15: Internet of Things (IoT) Security**

* **Lesson 15.1:** Overview of IoT Devices and Protocols
* **Lesson 15.2:** Common IoT Vulnerabilities
* **Lesson 15.3:** Attacking Embedded Systems
* **Lesson 15.4:** Firmware Analysis and Exploitation
* **Lesson 15.5:** Securing IoT Deployments

### **Module 16: Defensive Security and Countermeasures**

* **Lesson 16.1:** Intrusion Detection and Prevention Systems
* **Lesson 16.2:** Endpoint Security Solutions
* **Lesson 16.3:** Network Segmentation and Isolation
* **Lesson 16.4:** Security Information and Event Management (SIEM)
* **Lesson 16.5:** Incident Response Planning

### **Module 17: Penetration Testing Methodologies**

* **Lesson 17.1:** Planning and Scoping
* **Lesson 17.2:** Risk Assessment and Management
* **Lesson 17.3:** Execution of Penetration Tests
* **Lesson 17.4:** Reporting and Documentation
* **Lesson 17.5:** Presenting Findings to Stakeholders

### **Module 18: Legal and Regulatory Compliance**

* **Lesson 18.1:** Understanding Security Standards (PCI DSS, HIPAA)
* **Lesson 18.2:** Data Protection Laws and Regulations
* **Lesson 18.3:** Compliance Testing Procedures
* **Lesson 18.4:** International Cybersecurity Laws
* **Lesson 18.5:** Preparing for Audits

### **Module 19: Capture the Flag (CTF) and Practical Labs**

* **Lesson 19.1:** Introduction to CTF Competitions
* **Lesson 19.2:** Solving Real-World Challenges
* **Lesson 19.3:** Time Management and Strategy
* **Lesson 19.4:** Team Collaboration Techniques
* **Lesson 19.5:** Building Your Own CTF Challenges

### **Module 20: Career Development in Penetration Testing**

* **Lesson 20.1:** Building a Professional Portfolio
* **Lesson 20.2:** Certifications and Continuing Education
* **Lesson 20.3:** Networking and Community Involvement
* **Lesson 20.4:** Preparing for Technical Interviews
* **Lesson 20.5:** Staying Current with Industry Trends

————————

**Appendices**

* **Appendix A:** Glossary of Terms
* **Appendix B:** Recommended Reading and Resources
* **Appendix C:** Tool Installation Guides
* **Appendix D:** Sample Reports and Templates
* **Appendix E:** Practice Labs and Solutions

————————

This course provides a comprehensive journey from the fundamentals to advanced concepts in penetration testing and ethical hacking, focusing solely on technical skills and methodologies.

#security/pen-testing