Faysal Aziz

Mastering Ethical Hacking

A Comprehensive 5-Day CEH Certification Prep Course

FA-0304 · 5-Day

Software Development · DevOps, Cloud & Infrastructure · Cybersecurity

---

Introduction

Want to step into the world of ethical hacking? In this intensive 5-day course, you'll learn how to think like both attacker and defender – essential skills in a world where cyber threats grow more sophisticated by the day. You'll train for the globally recognized Certified Ethical Hacker (CEH) certification while getting your hands dirty with real-world hacking tools and techniques.

Your instructor brings three decades of cybersecurity experience to the classroom, showing you exactly how top organizations protect themselves from threats. This isn't just about passing an exam – you'll work through actual hacking scenarios, master the latest tools, and learn how to spot vulnerabilities before the bad guys do. By the end of the week, you'll be well-prepared for both the CEH v12 exam and the practical challenges of working as a penetration tester.**eal-world experience** in ethical hacking methodologies, tools, and countermeasures.

With over **30 years of industry experience**, the instructor will teach **practical, in-demand skills** required by top organizations today, moving beyond theoretical knowledge to real-world hacking scenarios.

Learning outcomes

By the end of this course, participants will be able to:

- **Understand the fundamentals** of ethical hacking, including legal and regulatory frameworks.
- **Conduct reconnaissance** using active and passive footprinting techniques.
- **Perform network scanning and enumeration** to identify vulnerabilities.
- **Exploit system vulnerabilities** and escalate privileges using hacking tools.
- **Analyze and mitigate malware threats, sniffing attacks, and social engineering tactics.**
- **Defend against Denial-of-Service (DoS) and session hijacking attacks.**
- **Evade firewalls, IDS/IPS, and honeypots** using advanced techniques.

🔹 **Assess and secure web applications, servers, and wireless networks.**
🔹 **Secure cloud computing, IoT devices, and mobile platforms** from cyber threats.
🔹 **Utilize cryptography** for secure communications and data protection.

Prerequisites

To get the most out of this course, participants should have:

✔ At least **two years of experience** in IT security, networking, or system administration.
✔ A **solid understanding of TCP/IP networking, Windows, and Linux/Unix systems.**
✔ **Basic knowledge of cybersecurity concepts** (e.g., CompTIA Security+ level).
✔ Familiarity with using **command-line interfaces and scripting** is helpful but not mandatory.

Training outline

1. 1. Introduction to Ethical Hacking

What is Ethical Hacking?

- White Hat vs. Black Hat vs. Grey Hat Hackers
- Cybersecurity Threat Landscape

Ethical Hacking Methodology

- The Five Stages of Hacking
- Cyber Kill Chain Framework

Legal and Ethical Considerations

- Compliance: GDPR, HIPAA, PCI-DSS
- Computer Fraud and Abuse Act, Ethical Hacking Laws
- Scope of Penetration Testing

2. 2. Footprinting and Reconnaissance

Information Gathering Techniques

- Passive vs. Active Footprinting
- OSINT (Open-Source Intelligence) Gathering

Tools for Footprinting

- WHOIS, Shodan, Maltego
- Google Dorking and Advanced Search Operators

DNS and Email Footprinting

- DNS Zone Transfers, MX Records, Subdomain Enumeration
- Email Header Analysis and Spoofing Detection

Social Engineering and Phishing

- Psychological Manipulation Tactics
- Phishing and Spear-Phishing Techniques

3. 3. Scanning Networks and Enumeration

Understanding Network Scanning

- Types of Scanning: TCP, UDP, SYN, ACK Scans
- Identifying Live Hosts and Open Ports

Tools for Network Scanning

- Nmap, Angry IP Scanner, Netcat

Enumerating Network Resources

- SMB, SNMP, LDAP, NetBIOS Enumeration
- Extracting User Credentials and Shares

Vulnerability Scanning

- Identifying Weak Services and Misconfigurations
- Automated Scanning with Nessus, OpenVAS

4. 4. Gaining and Maintaining Access

Exploiting System Vulnerabilities

- Buffer Overflows, SQL Injection, Command Injection
- Privilege Escalation Techniques

Using Exploitation Frameworks

- Metasploit, Empire, Cobalt Strike

Backdoor Creation and Persistence

- Trojans, Rootkits, Keyloggers
- Evading Antivirus and EDR Solutions

Session Hijacking and Credential Harvesting

- ARP Poisoning, DNS Spoofing
- Capturing Password Hashes with Mimikatz

5. 5. Malware Threats and Sniffing Attacks

Types of Malware and Attack Vectors

- Trojans, Ransomware, Spyware, Adware
- Zero-Day Exploits and Advanced Persistent Threats (APTs)

Packet Sniffing Techniques

- Man-in-the-Middle (MITM) Attacks
- Packet Capture with Wireshark

Detecting and Preventing Sniffing Attacks

- MAC Flooding, ARP Spoofing Prevention
- Encrypted Communications with SSL/TLS

6. 6. Denial-of-Service (DoS) and Web Application Attacks

Understanding DoS and DDoS Attacks

- Botnets and Amplification Attacks
- Tools: LOIC, HOIC, Slowloris

Web Application Security

- OWASP Top 10 Vulnerabilities
- Exploiting Cross-Site Scripting (XSS) and SQL Injection
- Web Server Security Best Practices

7. 7. Evading IDS, Firewalls, and Honeypots

Firewall and IDS/IPS Evasion Techniques

- Spoofing and Fragmentation Attacks
- Encryption and Tunneling Methods

Identifying and Bypassing Honeypots

- Detecting Deception Technologies

8. 8. Hacking Wireless Networks and IoT Devices

Wireless Network Vulnerabilities

- Cracking WEP/WPA2 with Aircrack-ng
- Rogue AP and Evil Twin Attacks

IoT Security Threats

- Smart Home and Industrial IoT Vulnerabilities

9. 9. Cloud and Mobile Security

Cloud Security Challenges

- Cloud Misconfigurations and Exploits
- Attacks on AWS, Azure, and Google Cloud

Mobile Security Vulnerabilities

- Mobile Malware, App Reverse Engineering

10. 10. Cryptography and Security Countermeasures

Understanding Encryption and Hashing

- Symmetric vs. Asymmetric Encryption
- Secure Hashing Algorithms (SHA, MD5)

- **Public Key Infrastructure (PKI) and Digital Signatures**
- **Steganography and Data Exfiltration Techniques**

Final Exam Preparation and Hands-On Lab

- **Exam Strategy and Time Management**
- **Practice Questions and Mock Exams**
- **Live Penetration Testing Challenges**
- **Q&A and Troubleshooting Session**

Why Take This Course?

Led by an expert with 30+ years of industry experience
Hands-on labs and real-world ethical hacking scenarios
Up-to-date with CEH v12 exam objectives
Practical skills that are highly sought after in the cybersecurity industry

By the end of this 5-day bootcamp, you'll be fully equipped to **pass the CEH exam** and confidently apply ethical hacking techniques in a professional setting.

Ready to become an **ethical hacker** and take your cybersecurity career to the next level? Let's get started!

© 2026 Faysal Aziz · Kuala Lumpur