CEHv10 Outline

EC-Council's Certified Ethical Hacker(CEH) course is meant to give the student a foundational knowledge and skillset to be an asset to their current organization as a security analyst or become an effective member of a security team engaged in offensive security testing and vulnerability assessments. In this course you'll learn about specific topics including: Intro to Ethical Hacking, Information gathering through foot-printing and reconnaissance techniques, network and system scanning, service enumeration, vulnerability discovery and analysis, system hacking, malware, social engineering, web application hacking, SQL Injection, Wireless, Mobile, IoT, and more.

==
1.0 Introduction
==

Module 01: Intro to Ethical Hacking

- Information Security Overview
- Information Security Threats and Attack Vectors
- Hacking Concepts
- Ethical Hacking Concepts
- Information Security Controls
- Penetration Testing Concepts
- Information Security Laws and Standards

==
2.0 Information Gathering and Vulnerability Identification
==

Module 02: Footprinting and Reconnaissance

- Footprinting concepts
- Footprinting through Search Engines
- Footprinting through Web Services
- Footprinting through Social Networking Sites
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Footprinting Countermeasures
- Footprinting Penetration Testing

Module 03: Scanning Networks

- Network Scanning Concepts
- Scanning Tools
- Scanning Techniques
- Scanning Beyond IDS and Firewall
- Banner Grabbing
- Draw Network Diagrams
- Scanning Pen Testing

Module 04: Enumeration

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP Enumeration
- SMTP and DNS Enumeration
- Other Enumeration Techniques

- Enumeration Countermeasures
- Enumeration Pen Testing

Module 05: Vulnerability Analysis

- Vulnerability Assessment Concepts
- Vulnerability Assessment Solutions
- Vulnerability Scoring Systems
- Vulnerability Assessment Tools
- Vulnerability Assessment Reports

==
3.0 Attacks and Exploits
==

Module 06: System Hacking

- System Hacking Concepts
- Cracking Passwords
- Escalating Privileges
- Executing Applications
- Hiding Files
- Covering Tracks
- Penetration Testing

Module 07: Malware Threats

- Malware Concepts
- Trojan Concepts
- Virus and Worm Concepts
- Malware Analysis
- Countermeasures
- Anti-Malware Software
- Malware Penetration Testing

Module 08: Sniffing

- Sniffing Concepts
- Sniffing Techniques: MAC Attacks
- Sniffing Techniques: DHCP Attacks
- Sniffing Techniques: ARP Poisoning
- Sniffing Techniques: Spoofing Attacks
- Sniffing Techniques: DNS Poisoning
- Sniffing Tools
- Countermeasures
- Sniffing Detection Techniques
- Sniffing Pen Testing

Module 09: Social Engineering

- Social Engineering Concepts
- Social Engineering Techniques
- Insider Threats
- Impersonation on Social Networking Sites
- Identity Theft
- Countermeasures
- Social Engineering Pen Testing

Module 10: Denial of Service

- DoS/DDoS Concepts
- DoS/DDoS Attack Techniques
- Botnets
- DDoS Case Study
- DoS/DDoS Attack Tools

- Countermeasures
- DoS/DDoS Protection Tools
- DoS/DDoS Penetration Testing

Module 11: Session Hijacking

- Session Hijacking Concepts
- Application Level Session Hijacking
- Network Level Session Hijacking
- Session Hijacking Tools
- Countermeasures
- Penetration Testing

Module 12: Evading IDS, Firewalls, and Honeypots

- IDS, Firewall, and Honeypot Concepts
- IDS, Firewall, and Honeypot Solutions
- Evading IDS
- IDS/Firewall Evading Tools
- Detecting Honeypots
- IDS/Firewall Evasion Countermeasures
- Penetration Testing

Module 13: Hacking Web Servers

- Web Server Concepts
- Web Server Attacks
- Web Server Attack Methodology
- Web Server Attack Tools
- Countermeasures
- Patch Management
- Web Server Security Tools
- Web Server Pen Testing

Module 14: Hacking Web Applications

- Web App Concepts
- Web App Threats
- Hacking Methodology
- Web App Hacking Tools
- Countermeasures
- Web App Security Testing Tools
- Web App Pen Testing

Module 15: SQL Injection

- SQL Concepts
- Types of SQL Injections
- SQL Injection Methodology
- SQL Injection Tools
- Evasion Techniques
- Countermeasures

Module 16: Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- Countermeasures
- Wireless Pen Testing

Module 17: Hacking Mobile Platforms

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Mobile Spyware
- Mobile Device Management
- Mobile Security Guidelines and Tools
- Mobile Pen Testing

Module 18: IoT Hacking

- IoT Concepts
- IoT Attacks
- IoT Hacking Methodology
- IoT Hacking Tools
- Countermeasures
- IoT Pen Testing

Module 19: Cloud Computing

- Cloud Computing Concepts
- Cloud Computing Threats
- Cloud Computing Attacks
- Cloud Security
- Cloud Security Tools
- Cloud Penetration Testing

Module 20: Cryptography

- Cryptography Concepts
- Encryption Algorithms
- Cryptography Tools
- Public Key Infrastructure
- Email Encryption
- Disk Encryption
- Cryptanalysis
- Countermeasures