

EC-Council Certified Ethical Hacker (CEH) v10.0

Overview

Students will learn how to scan, test, hack and secure target systems. The course covers the Five Phases of Ethical Hacking, diving into Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

Target Audience

Ethical hackers, System Administrators, Network Administrators and Engineers, Webmanagers, Auditors, Security Professionals in general.

Course Objectives

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

Course Outline

1 - Introduction to Ethical Hacking

- Overview of Current Security Trends
- Understanding Elements of Information Security
- Understanding Information Security Threats and Attack Vectors
- Overview of hacking concepts, types, and phases
- Understanding ethical hacking concepts and scope
- Overview of information security management and defense-in-depth
- Overview of policies, procedures, and awareness
- Overview of physical security and controls
- Understanding incidence management process
- Overview of vulnerability assessment and penetration testing
- Overview of information security acts and laws

[Register Online](#)

Schedule

Class Length: 5 Days

G2R = "Guaranteed to Run" | OLL = "Online LIVE"
ILT = "Instructor-Led-Training"

This course is not currently available on the public schedule. Please contact us using the information in the footer below to inquire about future dates or to schedule a private class.

2 - Footprinting and Reconnaissance

Understanding footprinting concepts
Footprinting through search engines
Footprint using advance google hacking techniques
Footprint through social networking sites
Understanding different techniques for website footprinting
Understanding different techniques for email footprinting
Understanding different techniques of competitive intelligence
Understanding different techniques for WHO IS footprinting
Understanding different techniques for network footprinting
Understanding different techniques of footprinting through social engineering
Footprinting tools
Footprinting countermeasures
Overview of footprinting Pen Testing

3 - Scanning Networks

Overview of networking scanning
Understanding different techniques to check for Live Systems
Understanding different techniques to check for Open Ports
Understanding various scanning techniques
Understanding various IDS Evasion Techniques
Understanding banner grabbing
Overview of Vulnerability scanning
Drawing network diagrams
Using Proxies and Anonymizer for attack
Understanding IP Spoofing and various detection techniques
Overview of scanning and Pen Testing

4 - Enumeration

Understanding Enumeration Concepts
Understanding different techniques for NetBIOS Enumeration
Understanding different techniques for SNMP enumeration
Understanding different techniques for LDAP enumeration
Understanding different techniques for NTP enumeration
Understanding different techniques for SMTP and DNS enumeration
countermeasures
Overview of enumeration pen testing

5 - Vulnerability Analysis

Vulnerability of the management life cycle
Understanding various approaches to vulnerability analysis
Tools used to perform the vulnerability assessments
Vulnerability analysis tools and techniques

6 - System Hacking

Overview of CEH Hacking Methodology
Understanding different techniques to gain access to the system
Understanding privilege escalation techniques
Understanding different techniques to create and maintain remote access to the system
Overview of different types of Rootkits
Overview of Steganography and Steganalysis
Understanding techniques to hide the evidence of compromise
Overview of system hacking penetration testing

7 - Malware Threats

Introduction to malware and malware propagation techniques
Overview of Trojans, their types, and how to infect systems
Overview of viruses, their types, and how they infect files
Introduction to computer worm
Understanding the Malware Analysis Process
Understanding different techniques to detect malware
Malware countermeasures
Overview of Malware penetration testing

8 - Sniffing

Overview of sniffing concepts
Understanding MAC attacks
Understanding DHCP attacks
Understanding ARP Poisoning
Understanding MAC Spoofing attacks
Understanding DNS poisoning
Sniffing tools
Sniffing countermeasures
Understanding various techniques to detect sniffing
Overview of sniffing Pen Testing

9 - Social Engineering

Overview of social engineering
Understanding various social engineering techniques
Understanding insider threats
Understanding impersonation on social networking sites
Understanding identity theft
Social engineering countermeasures
Identify theft countermeasures
Overview of Social Engineering Pen Testing

10 - Denial-of-Service

Overview of Denial of Service (DoS) and Distributed Denial-of-Service (DDoS)

Attacks

Overview different DoS/DDoS) attack techniques

Understanding the botnet network

Understanding various DoS and DDoS Attack Tools

DoS/DDoS Countermeasures

Overview of DoS Attack Penetration Testing

11 - Session Hijacking

Understanding session hijacking concepts

Understanding application level session hijacking

Understanding network level session hijacking

Session hijacking tools

Session hijacking countermeasures

Overview of session hijacking penetration testing

12 - Evading IDS, Firewalls, and Honeypots

Understanding IDS, Firewall, and honeypot concepts

IDS, Firewall and honeypot solutions

Understanding different techniques to bypass IDS

Understanding different techniques to bypass firewalls

IDS/Firewall evading tools

Understanding different techniques to detect honeypots

IDS/Firewall evasion countermeasures

Overview of IDS and firewall Penetration Testing

13 - Hacking Web Servers

Understanding webserver concepts

Understanding webserver attacks

Understanding webserver attack methodology

Webserver attack tools

Countermeasures against webserver attacks

Overview of Patch Management

Webserver security tools

Overview of Webserver penetration testing

14 - Hacking Web Applications

Understanding web application concepts

Understanding web application threats

Understanding web application hacking methodology

Web application hacking tools

Understanding web application countermeasures

Web application security tools

Overview of web application penetration testing

15 - SQL Injection

- Understanding SQL injection concepts
- Understanding various types of SQL injection attacks
- Understanding SQL injection methodology
- SQL injection tools
- Understanding different IDS evasion techniques
- SQL injection countermeasures
- SQL injection detection tools

16 - Hacking Wireless Networks

- Understanding wireless concepts
- Understanding wireless encryption algorithms
- Understanding wireless threats
- Understanding wireless hacking methodology
- Wireless hacking tools
- Understanding Bluetooth hacking techniques
- Understanding wireless hacking countermeasures
- Wireless security tools
- Overview of wireless penetration testing

17 - Hacking Mobile Platforms

- Understanding mobile attack platform vectors
- Understanding various android threat and attacks
- Understanding various iOS threats and attacks
- Understanding various Windows Phone OS threats and attacks
- Understanding various blackberry threats and attacks
- Understanding mobile device management (MDM)
- Mobile Security Guidelines and security tools
- Overview of Mobile Penetration Testing

18 - IoT Hacking

- Understanding IoT concepts
- Cryptography tools
- Understanding various IoT threats and attacks
- Understanding IoT Hacking
- Understanding IoT attacks
- IoT security Tools

19 - Cloud Computing

- Understanding Cloud Computing Concepts
- Understanding Cloud Computing Threats
- Understanding Cloud Computing Attacks
- Understanding Cloud Computing Security
- Cloud computing Security tools
- Overview of Cloud Penetration testing

20 - Cryptography

Understanding Cryptography concepts
Overview of encryption algorithms
Cryptography tools
Understanding Public Key Infrastructure (PKI)
Understanding email encryption
Understanding disk encryption
Understanding Cryptography attacks
Cryptanalysis Tools

Related Courses, Certifications, Exams _____

- EC Council Certified Ethical Hacking
 - EC0-350 - Certified Ethical Hacker Certification
 - 312-50 - Certified Ethical Hacker
-