Document Generated: 11/11/2026

Learning Style: On Demand

Technology: EC-Council

Difficulty: Intermediate

Course Duration: 40 Hours

Certified Ethical Hacker + Certification Exam



What's Included:

- *Official EC Council On-Demand curriculum*
- *Official EC Council Print or e-courseware included*
- *Official EC Council ilabs included*
- *EC Council Exam Voucher included*

The EC-Council Certified Ethical Hacker (CEH) certification is a globally recognized credential that validates your ability to identify, exploit, and secure vulnerabilities across modern systems and networks. This CEH online training offers a flexible, self-paced pathway for cybersecurity professionals and aspiring ethical hackers to build the technical foundation needed to detect, analyze, and defend against evolving cyber threats.

Through this CEH on demand course and using official EC-Council CEH course materials and hands-on virtual labs, students explore the five core phases of ethical hacking: reconnaissance, scanning, gaining access, maintaining access, and covering tracks. The program covers key topics such as penetration testing basics, network attack techniques, vulnerability analysis training, system hacking methodologies, and malware defense.

Certified Ethical Hackers are among the most sought-after professionals in cybersecurity. In the United States, CEH-certified experts earn an average annual salary of about **$100,000**, with experienced penetration testers and security analysts earning significantly more as they progress into senior or leadership roles.

Course Objectives:

This course will teach you the following:

- Top Information Security Attack Vectors
- Information Security Threat Categories
- Types of Attacks on a System
- Hacking Concepts, Types, and Phases
- Ethical Hacking Concepts and Scope
- Enumeration Concepts
- Enumeration Pen Testing
- CEH System Hacking Steps
- Spyware
- How to Defend Against Keyloggers
- Penetration Testing

Audience:

- This course is intended for: security officers, auditors, security professionals, site administrators and anyone concerned about the integrity of their

network infrastructure.

Prerequisites:

- You must have at least two years of experience in the field of information security to be able to take the CEH certification exam. The candidate must also have experience in IT in order to work professionally. For the most current requirements please check the eligibility requirements on the EC-Council website.

Course Outline:

Module 1: Introduction to Ethical Hacking

Module 2: Foot Printing and Reconnaissance

Module 3: Scanning Networks

Module 4: Enumeration

Module 5: Vulnerability Analysis

Module 6: System Hacking

Module 7: Malware Threats

Module 8: Sniffing

Module 9: Social Engineering

Module 10: Denial-of-Service

Module 11: Session Highjacking

Module 12: Evading IDS, Firewalls, and Honeypots

Module 13: Hacking Web Servers

Module 14: Hacking Web Applications

Module 15: SQL Injection

Module 16: Hacking Wireless Networks

Module 17: Hacking Mobile Platforms

Module 18: IoT and OT Hacking

Module 19: Cloud Computing

Module 20: Cryptography

Credly Badge:



Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges