QuickStart
Over 35 Years Of Technology Training

Document Generated: 12/18/2025

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*

About this Course:

Hackers are professionals at attacking systems and programs with weak security. In order to protect your systems from hackers, it is important that you learn the trick of the trade. The Certified Ethical Hacker program offered by us is a one-of-a-kind digital course, allowing professionals in the field to utilize their skills and knowledge in an efficient manner.

This hacking is ethical because you hack your own systems to find out about weakened security points in the system so you can fix it. From problem detecting to working on security loopholes, this training program gives you in-depth knowledge shared by certified professionals. This extensive security course is designed to secure systems from hackers who are often responsible for inconsolable loss for the organization.

Instead of leaving your system and network open to such malicious threats, it is best to learn technical information through this course. Some of the important areas covered in this course include virus creation and buffer overflows, DDOS Attacks, Social Engineering, and more. In short, this cyber security training program is ideal for those wanting to pass the Certified Ethical Hacker exam. Each component of the course is laid out in a manner that students can easily understand and practice the information provided. The course teaches individuals to adopt a defensive approach towards each attack or security breach.

This course revolves around thoroughly teaching the five phases of ethical hacking including gaining access, maintaining access, reconnaissance, track covering, and enumeration. Learning how to improve security of your systems by hacking into them each time is what we teach extensively in this course. After completion of this digitally advanced course, you will be able to enter the industry as an Information Security Engineer, Security Analyst, Security Consultant, Network Engineer, Penetration Tester, and many more.

If you are even slightly confused about taking this course, know that an Ethical Hacker earns an average of $100,000 annually.

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.

te.

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