

Certified Ethical Hacker (CEHv12)

Modality: Virtual Classroom

Duration: 5 Days

About this course:

Hacking involves professionals who attack your systems and programs that have weak security. The only way to protect your system from hackers is to learn the techniques to prevent it. The Certified Ethical Hacking Certification online is a unique course for individuals who are interested in utilizing this skill and knowledge for the betterment of corporations.

Ethical Hacking is different from normal hacking as this method teaches you how to hack your own systems in order to find loopholes in the security points. This course will teach you how to fix the system that is affected by these hackers. Plus after completing this Ethical Hacking course you will be able to keep your system files secure from any potential hacking threats to your organization.

Through Certified Ethical Hacking online, you will learn ways to keep your system secured from malicious threats. Moreover, anyone who applies for the CHFI program gets access to learn more about DDOS Attacks, Buffer Overflows, Virus Creation and Social Engineering. Without taking this course, candidates cannot appear for the CEH exam. The course is carefully laid out in a way so students can understand and apply these concepts in practice sessions. Through this, course students learn defensive strategies to stop systems from being attacked by hackers and other intrusions.

This course focuses on five aspects of ethical hacking including gaining access, maintaining access, reconnaissance, track covering and enumeration. Successfully completing this course online will help you enter the industry as an Information Security Engineer, Security Analyst, Security Consultant, IT Professional, Network Engineer, Penetration Tester, and many other similar job roles.

If you are still uncertain about opting for this course, just know that an Ethical Hacker can earn up to **\$100,000** per annum.

Certified Ethical Hacking is an InfoSec certification that prepares you for jobs like:

JOB TITLE	AVERAGE SALARY
Penetration Tester	\$88000
Cyber Security Engineer	\$103000
Information Security Manager	\$114000
Security Analyst	\$74000
Cyber Security Analyst	\$85000

Information Security Analyst **\$78000**

Security Engineer **\$91000**

Course Objective:

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 for candidates who are Security Officers, Auditors, Security Professionals, Site Administrators and those who have an interest in the integrity of network infrastructure.

Prerequisite:

- At least 2 years of experience in Information Security is needed to appear for the CEH certification exam. It is also required that the candidate must have a degree in an IT-related field in order to work full time. Be sure to check out the latest eligibility criteria on the EC Council Website.

Course Outline:

- **Module 1: Introduction to Ethical Hacking**
- **Module 2: Footprinting 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 Hijacking**
- **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 & OT Hacking**
- **Module 19: Cloud Computing**
- **Module 20: Cryptography**