Certified Ethical Hacker + Exam

**Overview**

This class will immerse the students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defences work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this intensive 5-day class they will have hands on understanding and experience in Ethical Hacking.

This course prepares you for the latest EC-Council Certified Ethical Hacker exam. Ethical Hacking and Countermeasures course’s mission is to educate, introduce and demonstrate hacking tools for penetration testing purposes only.

Prior to attending this course, you will be asked to sign an agreement stating that you will not use the newly acquired skills for illegal or malicious attacks and you will not use such tools in an attempt to compromise any computer system, and to indemnify EC-Council with respect to the use or misuse of these tools, regardless of intent.

**Target Audience**

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

**PreRequisites**

Knowledge and experience on the level of the following is advised:

* Microsoft MCSA/MCSE
* Network+
* Cisco CCNA

**Upon completing the course, you will be able to:**

* Understand the working of perimeter defences.
* How to scan and attack your own networks
* Understand how intruders escalate privileges
* Which steps to take to secure a system
* How to detect intrusion
* Create policies
* Learn about Social Engineering
* Learn about DDos Attacks, Buffer Overflows and Virus Creation

**Course contents**

Module 01: Introduction to Ethical Hacking

Module 02: Footprinting and Reconnaissance

Module 03: Scanning Networks

Module 04: Enumeration

Module 05: System Hacking

Module 06: Trojans and Backdoors

Module 07: Viruses and Worms

Module 08: Sniffers

Module 09: Social Engineering

Module 10: Denial of Service

Module 11: Session Hijacking

Module 12: Hijacking Webservers

Module 13: Hacking Web Applications

Module 14: SQL Injection

Module 15: Hacking Wireless Networks

Module 16: Evading IDS, Firewalls, and Honeypots

Module 17: Buffer Overflow

Module 18: Cryptography

Module 19: Penetration Testing

**Practical information**

The Certified Ethical Hacker exam 312-50 may be taken on the last day of the training (optional). Students need to pass the online Prometric exam to receive CEH certification.

Not anyone can be a student — the Accredited Training Centers (ATC) will make sure the applicants work for legitimate companies.