

# **EC-Council - Certified Ethical Hacker v6**

**Format:** Classroom

**Duration:** 5 Days

## **Description**

Hacking involves creativity and thinking 'outside-of-the-box', that is why vulnerability testing and security audits will not ensure the security proofing of an organization. To ensure that organisations have adequately protected their information assets, they must adopt the approach of 'defence in depth'. In other words, they must penetrate their networks and assess the security posture for vulnerabilities and exposure.

## **Objective**

The goal of the Ethical Hacking & Countermeasures Course is to teach a delegate to help his organization to take pre-emptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits. Delegates should be prepared for action paced course and the sheer size of the course content, however do not be intimidated as we will release e-learning prior to the delegate attending the course and also the instructor will prepare them thoroughly for the Certification Examination, the manuals can then be taken home and to work and can be used as excellent reference volumes.

Students will be encouraged to experiment and explore in our State-of-the-art Labs knowing that they will not compromise their Organisations network.

## **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**

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

## **Certification**

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.

## **Contents**

Module 1: Introduction to Ethical Hacking

Module 2: Footprinting

Module 3: Scanning

Module 4: Enumeration

Module 5: System Hacking

Module 6: Trojans and Backdoors

Module 7: Sniffers  
Module 8: Denial of Service  
Module 9: Social Engineering  
Module 10: Session Hijacking  
Module 11: Hacking Web Servers  
Module 12: Web Application Vulnerabilities  
Module 13: Web-based Password Cracking Techniques  
Module 14: SQL Injection  
Module 15: Hacking Wireless Networks  
Module 16: Virus  
Module 17: Physical Security  
Module 18: Linux Hacking  
Module 19: Evading IDS, Firewalls, and Honeypots  
Module 20: Buffer Overflows  
Module 21: Cryptography  
Module 22: Penetration Testing  
Module 23: Advanced Exploit Writing  
Module 24: Advanced Covert Hacking Techniques  
Module 25: Advanced Virus Writing Techniques  
Module 26: Advanced Reverse Engineering Techniques

### **Self Study Modules**

Covert Hacking Writing Virus Codes Assembly Language Tutorial Exploit Writing  
Smashing the Stack for Fun and Profit Windows Buffer Overflow Exploit Writing Reverse  
Engineering

### **Legal Agreement**

Ethical Hacking and Countermeasures course 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.