



## 1.1 CERTIFIED ETHICAL HACKING

### Certified Ethical Hacking (CEHv9)

CEHv9 is a comprehensive Ethical Hacking and Information Systems Security Auditing program focusing on latest security threats, advanced attack vectors, and practical real time demonstration of the latest Hacking Techniques, methodologies, tools, tricks, and security measures. Unlike other strictly theoretical training, you will be immersed in interactive sessions with hands-on labs after each topic.

Trainees will be able to explore their newly gained knowledge right away in their classroom by pentesting, hacking and securing your own systems. The lab intensive environment gives you in-depth knowledge and practical experience with the current, essential security systems. They will first begin with understanding how perimeter defenses work and then move into scanning and attacking networks, of course, no real network is harmed.

Trainees will also learn how intruders escalate privileges and what steps can be taken to secure a system. They will also gain knowledge about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows, and Virus Creation. At the end of this 5-day intensive training, participants will have hands on understanding and experience in Ethical Hacking. This course prepares participants for EC-Council Certified Ethical Hacker exam 312-50.

Module 01 Introduction to Ethical Hacking  
Module 02 Footprinting and Reconnaissance  
Module 03 Scanning Networks  
Module 04 Enumeration  
Module 05 System Hacking  
Module 06 Malware Threats  
Module 07 Sniffers  
Module 08 Social Engineering  
Module 09 Denial of Service  
Module 10 Session Hijacking  
Module 11 Hacking Webservers  
Module 12 Hacking Web Applications  
Module 13 SQL Injection  
Module 14 Hacking Wireless Networks  
Module 15 Hacking Mobile Platforms  
Module 16 Evading IDS, Firewalls, and Honeypots  
Module 17 Cloud Computing  
Module 18 Cryptography

### Who should Attend?

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