

Certified Ethical Hacker(CEH)

Exam 312-50



About the Program

Our security experts have designed over 140 labs which mimic real time scenarios in the course to help you “live” through an attack as if it were real and provide you with access to over 2200 commonly used hacking tools to immerse you into the hacker world.

As “a picture tells a thousand words”, our developers have all this and more for you in over 1685 graphically rich, specially designed slides to help you grasp complex security concepts in depth which will be presented to you in a 5 day hands on class by our Certified EC-Council Instructor.

The goal of this course is to help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation. You walk out the door with ethical hacking skills that are highly in demand, as well as the internationally recognized Certified Ethical Hacker certification! This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

What is New in CEH Version 9 Course

- Focus on New Attack Vectors
 - Emphasis on Cloud Computing Technology
 - CEHv9 focuses on various threats and hacking attacks to the emerging cloud computing technology
 - Covers wide-ranging countermeasures to combat cloud computing attacks
 - Provides a detailed pen testing methodology for cloud systems to identify threats in advance
 - Emphasis on Mobile Platforms and Tablet Computers
 - CEHv9 focuses on the latest hacking attacks targeted to mobile platform and tablet computers and covers countermeasures to secure mobile infrastructure
 - Coverage of latest development in mobile and web technologies
- New Vulnerabilities Are Addressed
 - Heartbleed CVE-2014-0160
 - Heartbleed makes the SSL layer used by millions of websites and thousands of cloud providers vulnerable.
 - Detailed coverage and labs in Module 18: Cryptography.
 - Shellshock CVE-2014-6271
 - Shellshock exposes vulnerability in Bash, the widely-used shell for Unix-based operating systems such as Linux and OS X.
 - Detailed coverage and labs in Module 11: Hacking Webservers
 - Poodle CVE-2014-3566
 - POODLE lets attackers decrypt SSLv3 connections and hijack the cookie session that identifies you to a service, allowing them to control your account without needing your password.
 - Case study in Module 18: Cryptography

Certified Ethical Hacker(CEH)

Exam 312-50

- Hacking Using Mobile Phones
 - CEHv9 focuses on performing hacking (Foot printing, scanning, enumeration, system hacking, sniffing, DDoS attack, etc.) using mobile phones
 - Courseware covers latest mobile hacking tools in all the modules
- Coverage of latest Trojan, Virus, Backdoors
- Courseware covers Information Security Controls and Information
- Security Laws and Standards
- Labs on Hacking Mobile Platforms and Cloud Computing
- More than 40 percent new labs are added from Version 8
- More than 1500 new/updated tools
- CEHv9 program focuses on addressing security issues to the latest operating systems like Windows 8.1
- It also focuses on addressing the existing threats to operating environments dominated by Windows 7, Windows 8, and other operating systems (backward compatibility)

Who Is It For?

The Certified Ethical Hacking training course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.