EC-Council CEH Day

Length: 7 days
Format: Classroom
Time: Day

About This Course

A Certified Ethical Hacker (CEH) is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

This primary goal of this course is to help each student pass the exams required to earn the CEH certification. To do this,Â your knowledgeableÂ instructor will blend hands-on labs with lecture and practice exams to prepare you to pass the exams. The practice exams identify knowledge gaps that the instructor will fill with customized, hands-on labs and tailored lectures.Â

To learn more about the course objectives and opportunities in the industry for CEH certified professionals, view our CEH Certification Info Session.

Required Exams

312-50 : Certified Ethical Hacker (CEH)

Audience Profile

This course is intended for students seeking to earn their CEH certification and who need an expert instructor to guide them throughout the training and exam preparation process. The CEH certification is for:

* Security OfficersÂ
* AuditorsÂ
* Network AdministratorsÂ Â
* Firewall AdministratorsÂ Â Â
* Security Professionals

Anyone who is concerned about the integrity of theÂ network infrastructure

Course Objectives

This course will cover the following topics:

* 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

* 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 10, Windows 7, Windows 8, and other operating systems (backward compatibility)

Outline

Module 1: Introduction to Ethical Hacking

Module 2: Footprinting and Reconnaissance

Module 3:Â System Hacking

Module 4: Malware Threats

Module 5: Scanning Networks

Module 6: Enumeration

Module 7: SniffiÂ-ng

Module 8: Social Engineering

Module 9: Denial of Service

Module 10: Session Hijacking

Module 11: SQL Injection

Module 12: Hacking Wireless Networks

Module 13:Â Hacking Web servers

Module 14: Hacking Web Applications

Module 15: Hacking Mobile Platforms

Module 16: Evading IDS, Firewalls, and Honeypot

Module 17: Cloud Computing