Certified Ethical Hacker (C|EH) v12

Why CEH Certifications ?

CEH stands for Certified Ethical Hacker, and it is arguably the best known of all the available EC-Council certifications. It was designed to indicate that the holder understands how to look for weaknesses and vulnerabilities in computer systems and is proficient with the tools used by a malicious hacker.

Training Solutions:

√ Offline Classroom Instructor-Led Training in our labs or onsite Locations.

√ Virtual Instructor-Led Training Via Virtual Video Conferencing Tools.

Why Learners Prefer CLS as their Training Services provider ?

■ Premuim Training Services Accredited from Global Technology Vendors.

■ Best Rated Experts & Certified Trainers in Egypt.

■ Official Training Hours, Practice Labs, Hands-on Learning.

■ CLS Training Classrooms are designed with High Edge PCs and Training Facilities.

■ Return on Training Investment is Guaranteed to boost performance.

Overview:

The Certified Ethical Hacker term was initially used to describe someone who possessed the skills necessary to be a hacker but whose moral code constrains them to stay within the bounds of legal activity. Over the years, the term ethical hacker has come to include all security professionals that provide offensive services, whether red team, pentester, or freelance offensive consultant.

The EC-Council organization certifies professionals in various e-business and security skills and knowledge. Their stated mission is to validate information security professionals who are equipped with the necessary skills and knowledge required in a specialized information security domain that will help them avert a cyber conflict, should the need ever arise.

CEH v12 Outline:
- Module 1: Introduction to Ethical HackingAnalytics
- Module 2: Footprinting and Reconnaissance
- Module 3: Scanning Networks
- Module 4: Enumeration
- Module 5: Vulnerability Analysis
- Module 6: System Hacking
- Module 7: Malware Threats
- Module 8: Sniffing
- Module 9: Social Engineering
- Module 10: Denial-of-Service
- Module 11: Session Hijacking
- Module 12: Evading IDS, Firewalls, and Honeypots
- Module 13: Hacking Web Servers
- Module 14: Hacking Web Applications
- Module 15: SQL Injection
- Module 16: Hacking Wireless Networks
- Module 17: Hacking Mobile Platforms
- Module 18: IoT and OT Hacking
- Module 19: Cloud Computing
- Module 20: Cryptography

Course Objectives:
- Information security controls, laws, and standards
- Various types of footprinting, footprinting tools, and countermeasures
- System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities
- Social engineering techniques and how to identify theft attacks to audit human-level vulnerabilities and social engineering countermeasures
- DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures
- Web application attacks, comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.

Audience Profile :

Who Needs CEH Certification?

Holding a CEH certification indicates the holder has acquired essential skills required to work in the following roles, among others:
- Security Analyst
- Computer Forensics Analyst
- Security Specialist
- Penetration Tester
- Security Engineer
- Security Code Auditor
- Malware Analyst
- Security Consultant

Prerequisities:

A candidate must meet one of the following criteria to be eligible to take the examination:

- Suppose the candidate is under the age of 18. In that case, the candidate is not eligible to attend an official training course or attempt the certification exam unless they provide written consent from their parent or legal guardian and a supporting letter from their nationally accredited institution of higher learning.