Certified Ethical Hacker (CEH v11)

The Certified Ethical Hacker (CEH) provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so you will be better positioned to setup your security infrastructure and defend against future attacks. An understanding of system weaknesses and vulnerabilities helps organizations strengthen their system security controls to minimize the risk of an incident. CEH was built to incorporate a hands-on environment and systematic process across each ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to achieve the CEH credential. You will be exposed to an entirely different posture toward the responsibilities and measures required to be secure. Now in its 11th version, CEH continues to evolve with the latest operating systems, tools, tactics, exploits, and technologies.

CEH is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is recognized as a standard within the information security community

The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: “To beat a hacker, you need to think like a hacker.”

How you’ll benefit

This class will help you:

- CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so that you will be better positioned to set up your security infrastructure and defend future attacks.
- Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident.
- Prepare you for the CEH exam

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10%
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs Run up to Date Code for all our courses

Certified Ethical Hacker (CEH v11)

Objectives

Upon completing this course, the student will be able to meet these objectives:

- Key issues plaguing the information security, network security, and computer forensics
- Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards.
- Perform footprinting and reconnaissance using the latest footprinting techniques and tools as a critical pre-attack phase required in ethical hacking.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- Vulnerability analysis to identify security loopholes in the target organization’s network, communication infrastructure, and end systems.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.
- Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.
- Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.
- Social engineering techniques and how to identify theft attacks to audit human-level vulnerabilities and suggest social engineering countermeasures.
- DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.
- Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.
- Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.
- Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.
- SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.
- Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
- Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.
- Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security techniques and tools.
- Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.

Course Duration

5 day

Course Price

$3,995.00

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Certification Exam

312-50

- Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
- Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.

Who Should Attend

The job roles best suited to the material in this course are:

- Information Security Analyst / Administrator
- Information Assurance (IA) Security Officer
- Information Security Manager / Specialist
- Information Systems Security Engineer / Manager
- Information Security Professionals / Officers
- Information Security / IT Auditors
- Risk / Threat/Vulnerability Analyst
- System Administrators
- Network Administrators / Engineers

AGE REQUIREMENTS AND POLICIES CONCERNING MINORS

- The age requirement for attending the training or attempting the CSCU exam is restricted to any candidate that is at least 13 years old.
- If the candidate is under the age of 13, they are not eligible to attend the official training or eligible to attempt the certification exam unless they provide the accredited training center (ATC) or EC-Council a written consent of their parent or their legal guardian and a supporting letter from their institution of higher learning. Only applicants from nationally accredited institutions of higher learning shall be considered.

Disclaimer

- EC-Council reserves the right to impose additional restriction to comply with the policy. Failure to act in accordance with this clause shall render the authorized training center (ATC) in violation of their agreement with EC-Council. EC-Council reserves the right to revoke the certification of any person in breach of this requirement.

Perquisites

To fully benefit from this course, you should have the following knowledge:

- Two years of security-related experience and a strong practical working knowledge of TCP/IP

Certified Ethical Hacker (CEH v11)

Outline

Module 01: Introduction to Ethical Hacking

Module 02: Footprinting and Reconnaissance

Module 03: Scanning Networks

Module 04: Enumeration

Module 05: Vulnerability Analysis

Module 06: System Hacking

Module 07: Malware Threats

Module 08: Sniffing

Module 09: 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