EC-Council

CEHv12: Certified Ethical Hacker (CEH) v12

$3,599.00

- 5 Days
- Over 220 hands-on labs!
- Pre-loaded with over 3,500 hacking tools
- Practice techniques and procedures in real-time on live machines
- This course includes one remote exam voucher for the CEH - Certified Ethical Hacker exam (312-50).

Upcoming Dates

Course Description

The Certified Ethical Hacker (CEH) credential 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. CEH v12 continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used by hackers and information security professionals today. 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.”

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.

CEH was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure.

In its 12th version, CEH continues to evolve with the latest operating systems, tools, tactics, exploits, and technologies.

This course includes one remote exam voucher for the CEH – Certified Ethical Hacker exam (312-50).

Course Outline

Module 01: Introduction to Ethical Hacking

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Module 02: Foot Printing and Reconnaissance

Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.

Module 03: Scanning Networks

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Module 04: Enumeration

Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, plus associated countermeasures.

Module 05: Vulnerability Analysis
Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems.

Module 06: System Hacking
Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

Module 07: Malware Threats
Get an introduction to the different types of malware, such as Trojans, viruses, and worms, as well as system auditing for malware attacks, malware analysis, and countermeasures.

Module 08: Sniffing
Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Module 09: Social Engineering
Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

Module 10: Denial-of-Service
Learn about different Denial-of-Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Module 11: Session Hijacking

Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Module 12: Evading IDS, Firewalls, and Honeypots

Get introduced to firewall, intrusion detection system, and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Module 13: Hacking Web Servers

Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Module 14: Hacking Web Applications

Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

Module 15: SQL Injection

Learn about SQL injection attack techniques, injection detection tools, and countermeasures to detect and defend against SQL injection attempts.

Module 16: Hacking Wireless Networks

Learn about wireless encryption, wireless hacking methodologies and tools, and Wi-Fi security tools

Module 17: Hacking Mobile Platforms

Learn about mobile platform attack vectors, Android vulnerability exploits, and mobile security guidelines and tools.

Module 18: IoT and OT Hacking

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Module 19: Cloud Computing

Learn different cloud computing concepts, such as container technologies and server less computing, various cloud-based threats and attacks, and cloud security techniques and tools.

Module 20: Cryptography

In the final module, learn about cryptography and ciphers, public-key infrastructure, cryptography attacks, and cryptanalysis tools.

Audience

Prerequisites

Students must have at least one year of hands-on experience in computer security. Students must also have a strong understanding of TCP/IP networking and modern operating systems. Certifications recommended prior to attending this class include A+, Security+, and Network+.

What You Will Learn

- Unique Learn, Certify, Engage and Compete Methodology for Aspiring Cyber Professionals
- Learn Ethical Hacking in a Structured Setting Across 20 Domains
- Build Skills With over 220 Challenge-Based, Hands-On Labs with CyberQ™ Labs
- Gain Experience With over 500 Unique Attack Techniques
- Learn Commercial-Grade Hacking Tools and Techniques
- Engage: “Hack” a Real Organization With C|EH® Elite to Get Experience
- Compete With Hackers Around the World as Part of the C|EH® Elite Program
- Attain the Most Recognized Credential in the Cybersecurity Industry :C|EH®