EC-Council

CEHv13: Certified Ethical Hacker (CEH) v13

$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

Mar 10 - Mar 14

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 v13 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 13th version, CEH continues to evolve with the latest operating systems, tools, tactics, exploits, and technologies.

The CEH v13 program immerses you in real-world ethical hacking through the dynamic CEH practice environment. With CEH Engage, you’ll sharpen your skills and prove you have what it takes to thrive as an ethical hacker.

New to CEH v13, learners will embark on their first emulated ethical hacking engagement. This four-phase engagement requires students to think critically and test the knowledge and skills gained by capturing a series of flags in each phase. It demonstrates the live application of skills and abilities in a consequence-free environment through EC-Council’s new “Cyber Range.”

As you complete your training and labs, CEH Engage empowers you to put theory into practice through a mock hacking engagement. You'll navigate a real-world, four-part engagement, targeting an emulated organization. Using a capture-the-flag format, you'll progress by answering critical "flag" questions, gaining hands-on experience in a full-scale ethical hacking operation.

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

Course Outline

Module 01: Introduction to Ethical Hacking

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

Module 02: Footprinting and Reconnaissance

Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking.

Module 03: Scanning Networks

Learn different network scanning techniques and countermeasures.

Module 04: Enumeration

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

Module 05: Vulnerability Analysis
Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools are also included.

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

Module 07: Malware Threats
Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.

Module 08: Sniffing
Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus 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, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Module 11: Session Hijacking

Learn 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

Learn about firewalls, intrusion detection systems (IDS), 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 hacking methodology for auditing vulnerabilities in web applications and countermeasures.

Module 15: SQL Injection

Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.

Module 16: Hacking Wireless Networks

Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.

Module 17: Hacking Mobile Platforms

Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

Module 18: IoT Hacking

Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.

Module 19: Cloud Computing

Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools.

Module 20: Cryptography

Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, 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

With 20 cutting-edge modules, you'll gain the core skills needed to dominate the cybersecurity landscape. CEH isn't just keeping pace—it's leading the charge, evolving with the latest operating systems, exploits, tools, and hacking techniques to ensure you're always ahead of the curve.

Dive deep into the future of cybersecurity with training that integrates AI into all five phases of ethical hacking, reconnaissance and scanning to gaining access, maintaining access, and covering tracks. You'll harness the power of AI to supercharge your hacking techniques and disrupt AI systems—giving you 10x efficiency in your cybersecurity role.

CEH v13 isn't just a certification; it's a fully immersive experience. CEH combines comprehensive knowledge-based training with immersive hands-on labs to ensure a well-rounded learning experience. You'll engage with live targets, tools, and vulnerable systems in a controlled environment, building real-world skills that empower you to confidently apply your expertise in any scenario. Get ready to transform the way you hack and protect the digital world!