CEHv12

Certified Ethical Hacker

Please note: *A new concept has been implemented for the C|EHv12, which consists of the four levels 1-Learn, 2-Certify, 3-Engage and 4-Complete. The course described below and the associated exam represent the 1-Learn and 2-Certify levels. Further information can be found in our Certification Overview as well as in this C|EH brochure.*

The C|EH® v12 training program includes 20 modules that cover various technologies, tactics and procedures, providing aspiring ethical hackers with the core knowledge they need to succeed in cybersecurity.

The 12th version of the C|EH® is delivered through a carefully curated training curriculum, typically spanning five days, and continues to evolve to keep pace with the latest operating systems, exploits, tools and techniques.

The concepts covered in the training program are split 50/50 between knowledge-based training and hands-on application through our cyber offering. Each tactic discussed in the training is supported by step-by-step exercises conducted in a virtualized environment with live targets, live tools and vulnerable systems. Through our lab technology, each participant receives extensive hands-on practice to learn and apply their knowledge.

Course Contents

- Introduction to Ethical Hacking
- Foot Printing and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking
- Cloud Computing
- Cryptography

Target Group

This course will particularly benefit security officers, auditors, security experts, website administrators and anyone responsible for the security of network infrastructures.

Prerequisites

There are no specific prerequisites for the C|EH program, but at least 2 years of IT security experience is recommended before attending a C|EH training program and therefore this course.

Exam

Once you have completed the course and been evaluated by EC-Council, you will receive a voucher for the "Certified Ethical Hacker 312-50" exam, which you can take at a VUE test center at no additional cost.

CEHv12 Pro

The course price includes the **CEHv12 Pro** version, which includes the following

- electronic course materials and the next version of the electronic course materials
- exam voucher
- 3x exam retakes
- 5x ethical hacking video courses
- 6 months access to the official lab
- CEH Engage

This Course in the Web

You can find the up-to-date information and options for ordering under the following link: www.experteach-training.com/go/**ECCE**

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in an non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Training		Prices, excl. of V.A.T.
Classes in Germany	**5 Days**	**€ 3,995**
Online Training	**5 Days**	**€ 3,995**

Date/course venue — Course language German

24/06-28/06/24	HY Hamburg	16/09-20/09/24	HY Online
24/06-28/06/24	HY Online	16/12-20/12/24	HY Frankfurt
16/09-20/09/24	HY Frankfurt	16/12-20/12/24	HY Online

CEHv12

Status 04/24/2024

EC-Council

ExperTeach

Table of Contents

CEHv12 – Certified Ethical Hacker

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.

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.

Scanning Networks
Learn different network scanning techniques and countermeasures.

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

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.

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

Malware Threats
Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures.

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

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

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.

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

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

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

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

SQL Injection
Learn about SQL injection attacks, evasion techniques, and SQL injection countermeasures.

Hacking Wireless Networks
Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi sedcurity tools, and countermeasures.

Hacking Mobile Platforms
Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

IoT and OT Hacking
Learn different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures.

Cloud Computing
Learn different cloud computing concepts, such as container technologies and server less computing, various cloud computing threats, attacks, hacking methodology, and cloud security techniques and tools.

Cryptography
Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

ExperTeach Benelux B.V.
Ceresstraat 1· 4811 CA Breda· Phone: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach-training.com