Updated on 01/25/2024

Sign up

CEH™ v12 Certification Preparation Training : Learn & Certify

EDU-312-50

5 days (35 hours)

Presentation

The Certified Ethical Hacker (CEH™ v12) is a recognized and respected training course that every security professional will need. Since its inception in 2003, the Certified Ethical Hacker has been widely distributed around the world, it is a respected certification accredited in ANSI 17024 compliance, adding credibility and value to certified members.

Now in its 12th version, the course has been updated to bring you the tools and techniques used by hackers and security professionals to penetrate any information system.

This course will immerse you in the "Hacker mindset", with the aim of teaching you to think like a hacker in order to better defend yourself. In particular, you'll learn how to scan, test, hack and secure a targeted system. The course covers the Five Phases of Ethical Hacking: Reconnaissance, Gaining Access, Enumeration, Maintaining Access and Removing Traces.

The tools and techniques for each of these 5 phases are presented in great detail; no other training course will offer you as many learning resources, labs, tools and techniques as CEH™ v12.

Objectives

- Understanding the fundamentals of ethical hacking
- Have the skills to secure systems, networks, databases or applications from hacking attacks
- Ready for CEH™ certification

Target audience

This course is particularly aimed at security managers, auditors, security professionals, site administrators and anyone concerned with the stability of information systems.

Prerequisites

- Experience in using Windows and Linux operating systems
- Basic knowledge of TCP/IP network protocols and operation
- 2 years' experience in cybersecurity

Teaching methods

The CEH 312-50 exam can be taken on the last day of training. Students must take the exam on the ECC exam online platform, with the option of using ProctorU, or at a VUE test center to obtain certification.

Examination title: Certified Ethical Hacker (ANSI)Examination code: 312-50 (ECC EXAM), 312-50 (VUE)Number of questions: 125 : 4 hoursAvailability: ECCEXAM / VUE

Ambient IT is not an EC-Council© ATC. This official training is provided in partnership by Exclusive Networks, EC-Council©'s official ATC- Accredited Training Center, by an official trainer.

CEH™ Certification Preparation Program

Introduction

- Back to safety basics
- What is ethical hacking?
- What are the ethical hacker's missions?

Information gathering

- Footprinting
- TCP/IP networks
- Scanning method
- Listing

Attacking networks

- Wireless networking

- Network concepts
- Techniques and tools
- Escape techniques
- Wireless hacking

Hacking a system

- Authentication
- Elevation of privileges
- Hide files
- Covering your tracks
- Malware
- Denial of service
- Session hijacking
- Hacking a web application

Web servers

- Attack methodologies
- Web server architecture
- Server attacks
- Attacks on web applications

IoT

- Architecture
- The hacking method
- Vulnerabilities
- The attacks
- Mobile attacks and vulnerabilities

Cloud Computing

- Types of service
- The threats
- The attacks
- Cloud hacking

Cryptography

- A reminder of cryptography
- PKI
- Digital certificates
- Encrypted communications
- Cryptographic attacks

Pentest

- Security audit
- Active recognition
- The methodology
- Farms

Social Engineering

- Introduction to social engineering
- Protecting yourself against this type of attack
- Attacks on mobile devices vs. attacks on mobile devices
- Physical safety

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.