Certified Ethical Hacker (CEH) Training

Course: **00049**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Gouvernance, Risk and Compliance**
Price: **3000,00 €**

About Course

In this CEH training course, you are provided with the foundational knowledge needed to pass the EC-Council Certified Ethical Hacker (CEH v12) exam.

What you'll learn

- You will learn how to deploy tools and techniques to protect your network through hands-on labs that mimic real-life scenarios.

Pre-requisites

- Passing the CEH Certification Exam meets U.S. DoD Directive 8140/8570.01 CSSP Analyst, CSSP Infrastructure Support, CSSP Auditor, and CSSP Incident Responder requirements.

Curriculum

Module 1: Introduction to Ethical Hacking

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

Module 2: Foot Printing and Reconnaissance

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

Module 3: Scanning Networks

- Learning different network scanning techniques and countermeasures.

Module 4: Enumeration

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

Module 5: Vulnerability Analysis

- Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Use Different types of vulnerability assessment and vulnerability assessment tools

Module 6: System Hacking

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

Module 7: Malware Threats

- Learn distinct types of malware (Trojan, viruses, worms, etc.), APT (Advance Persistent Threat) and fileless malware, malware analysis procedure, and malware countermeasures.

Module 8: Sniffing

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

Module 9: Social Engineering

- Learn social engineering concepts and techniques, including identifying theft attempts, auditing human-level vulnerabilities, and suggesting social engineering countermeasures.

Module 10: Denial-of-Service

- Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques and 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 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 web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

Module 15: SQL Injection

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

Module 16: Hacking Wireless Networks

- Understand several wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi security tools, and countermeasures.

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 and OT Hacking

- Learn different types of IoT and OT attacks, hacking methodology, 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 methodology, 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.