Certified Ethical Hacker v11 Duration 5 Days

Overview

Who is a Certified Ethical Hacker?

A Certified Ethical Hacker is a specialist typically working in a red team environment, focused on attacking computer systems and gaining access to networks, applications, databases, and other critical data on secured systems. A CEH understands attack strategies, the use of creative attack vectors, and mimics the skills and creativity of malicious hackers. Unlike malicious hackers and actors, Certified Ethical Hackers operate with permission from the system owners and take all precautions to ensure the outcomes remain confidential. Bug bounty researchers are expert ethical hackers who use their attack skills to uncover vulnerabilities in the systems.

The CEHv11 course is now accredited under the NCSC Certified Training Scheme.

What's Included?

Included in our CEHv11 course:

CEHv11 (ANSI) Exam Voucher

CEHv11 iLabs (Post Course CEHv10 Lab Access - 6 months)

Prerequisites

Before attending this accelerated ethical hacking course, you should hold two years' IT work experience and possess a basic familiarity of Linux and/or Unix. We also recommend you possess a strong working knowledge of:

- TCP/IP
- Windows Server

Learners will not be able to access the EC Council CEHv11 course material until they receive their login details, which they are given on the first day of the course.

Learning Outcomes

- Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards.
- Perform footprinting and reconnaissance using the latest footprinting techniques and tools as a critical pre-attack phase required in ethical hacking.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.

- System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.
- Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.
- Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.
- Social engineering techniques and how to identify theft attacks to audit humanlevel vulnerabilities and suggest social engineering countermeasures.
- DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.
- Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.
- Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.
- Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.
- SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.
- Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
- Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.
- Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security techniques and tools.
- Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
- Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.

Course Outline

Module 01
Introduction to Ethical Hacking
Module 02
Footprinting and Reconnaissance
Module 03
Scanning Networks
Module 04
Enumeration

Module 05
Vulnerability Analysis
Module 06
System Hacking
Module 07
Malware Threats
Module 08

Sniffing

Module 09

Social Engineering

Module 10

Denial-of-Service

Module 11

Session Hijacking

Module 12

Evading IDS, Firewalls, and Honeypots

Module 13

Hacking Web Servers

Module 14

Hacking Web Applications

Module 15

SQL Injection

Module 16

Hacking Wireless Networks

Module 17

Hacking Mobile Platforms

Module 18

IoT and OT Hacking

Module 19

Cloud Computing

Module 20

Cryptography