Certified Ethical Hacker (C|EH) v10

Duration: 5 Days
Method: Instructor-Led Training (ILT)

Certification: Certified Ethical Hacker

Course Description

The Certified Ethical Hacker program is the most desired information security training program any information security professional will ever want to be in. To master the hacking technologies, participants will need to become one, but an ethical one! The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, "To beat a hacker, participants need to think like a hacker".

This course will immerse participants into the Hacker Mindset so that they will be able to defend against future attacks. The security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment.

This ethical hacking course puts participants in the driver's seat of a hands-on environment with a systematic process. Here, participants will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! Participants will scan, test, hack and secure their own systems. Participants will be taught the five phases of ethical hacking and the ways to approach their target and succeed at breaking in every time! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering their tracks.

Target Audience

This course is intended for:

- Auditors
- Ethical Hackers
- Network Administrators and Engineers
- Security Professionals in general
- Site Administrators
- System Administrators
- Web Managers
- Persons who is concerned about the integrity of the network infrastructure.

Prerequisites

To attend this course, participants should have:

- CND or CompTIA Security+ and Network+ certification or equivalent knowledge
- Practical industry experience in networking **(At least one (1) year)**
- Working knowledge of Linux
- Strong Microsoft Windows skills
- Good understanding of computer networking

Exam Details

Exam Tile:	•Certified Ethical Hacker (ANSI)
Exam Code:	•312-50
Length of Exam:	•4 Hours
Number of Questions:	•125
Availability:	•ECCEXAM Portal or VUE
Question Format:	•Multiple Choice Questions

- **NOTE:** ANSI — American National Standards Institute

Course Objectives

Upon successful completion of this course, participants will have learnt:

- Key issues plaguing the information security world, incident management process, and penetration testing.
- Various types of footprinting, footprinting tools, and countermeasures.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks.
- Different types of Trojans, Trojan analysis, and Trojan countermeasures.
- Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures.
- Packet sniffing techniques and how to defend against sniffing.
- Social Engineering techniques, identify theft, and social engineering countermeasures.
- DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures.
- Session hijacking techniques and countermeasures.
- Different types of webserver attacks, attack methodology, and countermeasures.
- Different types of web application attacks, web application hacking methodology, and countermeasures.
- SQL injection attacks and injection detection tools.
- Wireless Encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
- Mobile platform attack vector, android vulnerabilities, mobile security guidelines, and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures.
- Various cloud computing concepts, threats, attacks, and security techniques and tools.
- Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.
- Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
- Different threats to IoT platforms and learn how to defend IoT devices securely

Course Content

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 Hacking

Module 19: Cloud Computing

Module 20: Cryptography

LABS INCLUDED