BOOST
THE LEADING TRAINING PROVIDER

Information Technology

Certified Ethical Hacker v12 - CEHv12

Course Introduction

This Certified Ethical Hacker (CEH V12) training course is one of the most sought-after security qualifications in the world. This internationally recognized security course validates your ability to discover weaknesses in the organization's network infrastructure and aids in the effective combat of cyber-attacks. This training program is designed to introduce participants the essential concepts about ethical hacking with hands-on training, labs, assessment, a mock engagement (practice), and a global hacking competition.

Target Audience

- Cloud Computing Engineer
- Computer Network Specialist
- Computer Support Specialist
- Database Administrator
- Information Technology Analyst
- Information Technology Leadership
- Information Security Specialist
- Software/Application Developer
- Web Developer
- Technology sales consultant

Learning Objectives

- Ethical hacking fundamentals, cyber kill chain concepts, an overview of information security, security measures, and numerous information security laws and regulations.
- Enumeration techniques include NFS enumeration and related tools, DNS cache snooping, and DNSSEC Zone walking along with the countermeasures.

- Concepts of vulnerability assessment, its categories and strategies, and first-hand exposure to the technologies used in industry.
- Phases of system hacking, attacking techniques to obtain, escalate, and maintain access on the victim and covering tracks.
- Malware threats, analysis of various viruses, worms, and trojans like Emotet and battling them to prevent data. APT and Fileless Malware concepts have been introduced to this domain.
- Packet sniffing concepts, techniques, and protection against the same.
- Social engineering concepts and related terminologies like identity theft, impersonation, insider threats, social engineering techniques, and countermeasures.
- Security solutions like firewall, IPS, honeypots, evasion, and protection.
- Operational Technology (OT) essentials, threats, attack methodologies, and attack prevention. The concept of OT is a new addition.
- Recognizing the vulnerabilities in IoT and ensuring the safety of IoT devices.
- Encryption algorithms, Public Key Infrastructure (PKI), cryptographic attacks, and cryptanalysis.
- Cloud computing, threats and security, essentials of container technology, and serverless computing.

Course Outline

- **Day 01**
  - Module 01: Introduction to Ethical Hacking
  - Module 02: Foot Printing and Reconnaissance
  - Module 03: Scanning Networks
  - Module 04: Enumeration
- **Day 02**
  - Module 05: Vulnerability Analysis
  - Module 06: System Hacking
  - Module 07: Malware Threats
  - Module 08: Sniffing
- **Day 03**
  - Module 09: Social Engineering
  - Module 10: Denial-of-Service
  - Module 11: Session Hijacking
  - Module 12: Evading IDS, Firewalls, and Honeypots

- **Day 04**
  - Module 13: Hacking Web Servers
  - Module 14: Hacking Web Applications
  - Module 15: SQL Injection
  - Module 16: Hacking Wireless Networks
- **Day 05**
  - Module 17: Hacking Mobile Platforms
  - Module 18: IoT and OT Hacking
  - Module 19: Cloud Computing
  - Module 20: Cryptography

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
June 16, 2025	June 20, 2025	5 days	4250.00 $	UAE - Abu Dhabi
Sept. 8, 2025	Sept. 12, 2025	5 days	4950.00 $	Malaysia - kuala lumpur
Dec. 29, 2025	Jan. 2, 2026	5 days	2150.00 $	Virtual - Online
Sept. 1, 2025	Sept. 5, 2025	5 days	4250.00 $	UAE - Dubai
Sept. 8, 2025	Sept. 12, 2025	5 days	4250.00 $	UAE - Abu Dhabi