Certified Ethical Hacker (CEHV13)

Course Duration: 5 Days

Course Overview

The CEH v13 is a specialized, one-of-akind training program that helps you gain expertise in ethical hacking, AI, and machine learning. With hands-on training labs, knowledge-based and practical exams, a mock ethical hacking engagement on live networks, and a global hacking competition, this program ensures you master the most in-demand skills needed to excel and stand out in the cybersecurity industry. This learning framework offers not only a comprehensive training program to prepare you for the certification exam but also the industry's most robust, in-depth, hands-on lab and practice range experience.
The Certified Ethical Hacker has been battle-hardened over the last 20 years, creating hundreds of thousands of Certified Ethical Hackers employed by top companies, militaries, and governments worldwide. In its 12th version, the Certified Ethical Hacker provides comprehensive training, hands-on learning labs, practice cyber ranges for engagement, certification assessments, cyber competitions, and opportunities for continuous learning into one comprehensive program curated through our new learning framework:

1. Learn
2. Certify
3. Engage
4. Compete

A C|EH® 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.

Enter the Hackerverse™ With the C|EH® v12 Enhance Your Ethical Hacking Career

1. Learn:

- 20 modules
- 2500+ pages of student manual
- 2000 pages of lab manual
- Over 221 hands-on labs to practice attack vectors and hacking tools

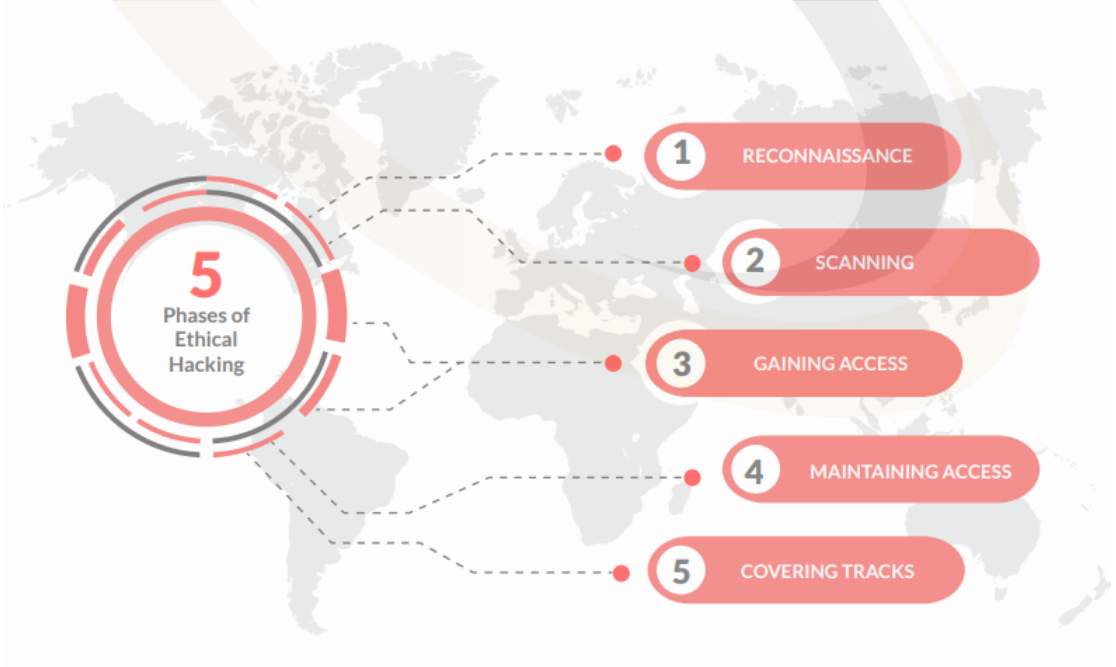
- AI integrated skills in the 5 phases of the ethical hacking framework
- Hacking AI system, based on the Top 10 OWASP vulnerabilities
- Over 4000 hacking and security tools
- Learn how to hack multiple operating systems (Windows 11, Windows servers, Linux, Ubuntu, Android)
- More than 50% of training time is dedicated to labs

2. Certify:

- Knowledge-Based Exam (ANAB ISO 17024 and US DoD 8140)
- 4 hours 125 multiple-choice questions
- Practical Exam (ANAB ISO 17024 and US DoD 8140)
- 6 hours 20 real scenario based questions

3. Engage

- 4000 hacking tools
- 550 attack techniques
- Conduct a real-world ethical hacking assignment
- Apply the 5 phases
  1. Reconnaissance
  2. Scanning
  3. Gaining access
  4. Maintaining access
  5. Covering your tracks



4. Compete:

- New challenges every month
- 4-hour CTF competition
- Compete with your peers worldwide

- Hack your way to the top of the leaderboard
- Focus on new attack vectors
- Exploit emerging vulnerabilities
- Challenges include:
  - Ransomware
  - Web app hardening
  - Unpatched software
  - System hacking
  - Service exploitation
  - Incident response
  - Forensic analysis
  - Web app hacking and pen testing
  - Reverse engineering
  - Cryptography
  - Encryption
  - Hacking cloud networks
  - ICS/SCAD

Who Should Attend?

- Security officers
- Auditors
- Security professionals
- Site administrators and anyone who is concerned about the integrity of the network infrastructure.

Course Outline:

Module #	Module Topic	Description
Module 01	Introduction to Ethical Hacking	Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures
Module 02	Foot Printing and Reconnaissance	Learn how to use the latest techniques and tools for foot printing and reconnaissance, a critical pre-attack phase of ethical hacking
Module 03	Scanning Networks	Learn different network scanning techniques and countermeasures.
Module 04	Enumeration	Learn various enumeration techniques, including Border

		Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures.
Module 05	Vulnerability Analysis	Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools are also included
Module 06	System Hacking	Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks.
Module 07	Malware Threats	Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.
Module 08	Sniffing	Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks
Module 09	Social Engineering	Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.
Module 10	Denial-of-Service	Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.
Module 11	Session Hijacking	Learn 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	Learn about 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 hacking methodology for auditing vulnerabilities in web applications and countermeasures.
Module 15	SQL Injection	Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.
Module 16	Hacking Wireless Networks	Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks
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 Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.
Module 19	Cloud Computing	Learn different cloud computing concepts, such as container technologies and server less 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.

Exam Details:

Exam Details	C|EH® (Knowledge Exam)	C|EH® (Practical Exam)
Number of Questions/Practical Challenges	125	20 Practical Challenges
Test Duration	4 Hours	6 Hours
Test Format	Multiple Choice Questions	iLabs Cyber Range
Test Delivery	ECC EXAM, VUE	iLabs Cyber Range
Exam Prefix	312-50 (ECC EXAM), 312-50 (VUE)	-
Passing Score	from 60 percent to 85 percent	60% - 85%