REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

Certified Ethical Hacker (C|EH) v13

Duration: 5 Days

Method: Instructor-Led Training (ILT) | Live Online Training

Certification: *Certified Ethical Hacker* — ***Exam:*** *312-50*

Course Description

The Certified Ethical Hacker (CEH) credential is one of the most trusted certifications in ethical hacking and is recommended by employers worldwide. Since 2003, it has been recognized as a key standard in the information security field. CEH covers the five (5) essential phases of ethical hacking through hands-on experience with modern technologies. Understanding these phases is vital for any organization, and the mission remains the same: "To beat a hacker, you need to think like a hacker."

In its thirteenth (13th) version, the course provides specialized training that helps participants develop skills in ethical hacking, artificial intelligence (AI), and machine learning. It includes hands-on labs, exams, a live ethical hacking simulation, and a global competition. This course ensures participants gain the top skills needed in cybersecurity. CEH v13 introduces a four (4) phase AI-driven learning framework:

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

CEH v13 is more than just a certification. It provides an immersive experience, combining knowledge with hands-on labs where participants work with real tools and systems in a controlled environment. By the end of the course, participants will master AI-driven cybersecurity, learn to hack AI systems, and improve their ability to protect the digital world.

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

Target Audience

This course is intended for:

- Cyber Defence Analysts
- Cybersecurity Analysts/Auditors/Consultants
- Information Security Administrators/Analysts/Auditors/Managers
- Infosec Security Administrators
- Network (Security) Engineers
- Security Administrators/Analysts
- Security Consultants
- SOC (Security) Analysts
- Solution Architects
- Vulnerability Assessment Analysts
- Warning Analysts.

Prerequisites

To attend this course, candidates must have:

- *Certified Network Defender (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 Code:	• 312-50
Length of Exam:	• 4 Hours
Number of Questions:	• 125
Passing Score:	• 70%
Question Format:	• Multiple Choice

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

Course Objectives

Upon successful completion of this course, attendees will be able to:

- Understand the fundamentals of ethical hacking and information security.
- Excel in techniques for footprinting, reconnaissance, network scanning, and enumeration.
- Conduct vulnerability analysis and system hacking to uncover security loopholes.
- Detect and defend against malware, sniffing, and social engineering attacks.
- Study and mitigate Denial-of-Service (DoS) and session hijacking attacks.
- Evade and audit IDS, firewalls, and honeypots.
- Secure web servers, web applications, wireless networks, and mobile platforms.
- Protect Internet of Things (IoT), operational technology (OT), and cloud environments.
- Implement cryptography and safeguard systems against cryptographic attacks.
- Explore and use AI-driven security tools for advanced cybersecurity practices.

Course Topics

Module 1: 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 2: Footprinting and Reconnaissance

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

Module 3: Scanning Networks

- Learn different network scanning techniques and countermeasures.

Module 4: Enumeration

- Learn various enumeration techniques, including 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. Different types of vulnerability assessment and vulnerability assessment tools are also included.

Module 6: 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.

Course Topics *Continued*

Module 7: Malware Threats

- Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.

Module 8: Sniffing

- Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.

Module 9: 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 (DoS)

- 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.

Course Topics *Continued*

Module 16: Hacking Wireless Networks

- Learn about different types of encryptions, 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: Internet of Things (IoT) and Operational Technology (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 serverless computing, various cloud computing threats, attacks, hacking methodologies, 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.

Appendix: Learn AI Tools

- Learn to use a range of advanced AI tools, including ShellGPT, ChatGPT, FraudGPT, WormGPT, DeepExploit, Nebula, Veed.io, and many more, to enhance their cybersecurity skills.

LABS INCLUDED