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

Certified Ethical Hacker (C|EH) v12

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 the most trusted ethical hacking certification and is recommended by employers globally. Since its introduction in 2003, it is recognized as a standard within the information security community. It provides comprehensive hands-on coverage of the five (5) phases of Ethical Hacking across a variety of current-day technologies. Knowing these five phases of ethical hacking is crucial to any organization, and the original core mission of CEH remains valid and relevant today: "To beat a hacker, you need to think like a hacker."

This course will enhance participants' knowledge of essential security fundamentals. It will also validate their ability to discover weaknesses in the organization's network infrastructure and aid in the effective combat of cyber-attacks. In its 12th version, the course 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.

The course also equips participants with the tactics, techniques, and procedures (TTPs) to build ethical hackers who can uncover weaknesses in nearly any type of target system before cybercriminals do.

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 have a thorough understanding of:

- Ethical hacking fundamentals, cyber kill chain concepts, an overview of information security, security measures, and numerous information security laws and regulations.
- Footprinting concepts and methodologies, as well as using footprinting tools and countermeasures.
- 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 the 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.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, use cases, and attack and defence tools.
- Security solutions like firewalls, 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.

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

Course Topics

Module 1: Introduction to Ethical Hacking

- Elements of Information Security
- Cyber Kill Chain Methodology
- MITRE ATT&CK Framework
- Hacker Classes
- Ethical Hacking
- Information Assurance (IA)
- Risk Management
- Incident Management
- PCI DSS
- HIPPA
- SOX
- GDPR

Module 2: Footprinting and Reconnaissance

- Footprinting Concepts
- Footprinting through Search Engines
- Footprinting through Web Services
- Footprinting through Social Networking Sites
- Website Footprinting
- Email Footprinting
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools
- Footprinting Countermeasures

Module 3: Scanning Networks

- Network Scanning Concepts
- Scanning Tools
- Host Discovery
- Port and Service Discovery
- OS Discovery (Banner Grabbing/OS Fingerprinting)
- Scanning Beyond IDS and Firewall
- Network Scanning Countermeasures

Module 4: Enumeration

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP and NFS Enumeration
- SMTP and DNS Enumeration
- Other Enumeration Techniques
- Enumeration Countermeasures

Module 5: Vulnerability Analysis

- Vulnerability Assessment Concepts
- Vulnerability Classification and Assessment Types
- Vulnerability Assessment Tools
- Vulnerability Assessment Reports

Module 6: System Hacking

- Gaining Access
- Escalating Privileges
- Maintaining Access
- Clearing Logs

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

Course Topics *Continued*

Module 7: Malware Threats

- Malware
- Components of Malware
- Advanced Persistent Threat (APT)
- Trojan
- Types of Trojans
- Exploit Kits
- Virus
- Virus Lifecycle
- Types of Viruses
- Ransomware
- Computer Worms
- Fileless Malware
- Malware Analysis
- Virus Detection Methods
- Trojan Analysis
- Virus Analysis
- Fileless Malware Analysis
- Anti-Trojan Software
- Antivirus Software
- Fileless Malware Detection Tools

Module 8: Sniffing

- Network Sniffing
- Wiretapping
- MAC Flooding
- DHCP Starvation Attack
- ARP Spoofing Attack
- ARP Poisoning
- ARP Poisoning Tools
- MAC Spoofing
- STP Attack
- DNS Poisoning
- DNS Poisoning Tools
- Sniffing Tools
- Sniffer Detection Techniques
- Promiscuous Detection Tools

Module 9: Social Engineering

- Social Engineering
- Types of Social Engineering
- Phishing
- Phishing Tools
- Insider Threats/Insider Attacks
- Identity Theft

Module 10: Denial-of-Service (DoS)

- DoS Attack
- Distributed DoS (DDoS) Attack
- Botnets
- DoS/DDoS Attack Techniques
- DoS/DDoS Attack Tools
- DoS/DDoS Attack Detection Techniques
- DoS/DDoS Protection Tools

Module 11: Session Hijacking

- Session Hijacking
- Types of Session Hijacking
- Spoofing
- Application-Level Session Hijacking
- Man-in-the-Browser Attack
- Client-side Attacks
- Session Replay Attacks
- Session Fixation Attack
- CRIME Attack
- Network Level Session Hijacking
- TCP/IP Hijacking
- Session Hijacking Tools
- Session Hijacking Detection Methods
- Session Hijacking Prevention Tools

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

Course Topics *Continued*

Module 12: Evading IDS, Firewalls, and Honeypots

- IDS, IPS, Firewall, and Honeypot Concepts and Solutions
- Evading IDS
- Evading Firewalls
- Evading NAC and Endpoint Security
- IDS/Firewall Evading Tools
- Detecting Honeypots
- IDS/Firewall Evasion Countermeasures

Module 13: Hacking Web Servers

- Web Server Operations
- Web Server Attacks
- DNS Server Hijacking
- Website Defacement
- Web Cache Poisoning Attack
- Web Server Attack Methodology
- Web Server Attack Tools
- Web Server Security Tools
- Patch Management
- Patch Management Tools

Module 14: Hacking Web Applications

- Web Application Architecture
- Web Application Threats
- OWASP Top 10 Application Security Risks – 2021
- Web Application Hacking Methodology
- Web API
- Webhooks and Web Shell
- Web API Hacking Methodology
- Web Application Security

Module 15: SQL Injection

- SQL Injection
- Types of SQL injection
- Blind SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- Signature Evasion Techniques
- SQL Injection Detection Tools

Module 16: Hacking Wireless Networks

- Wireless Terminology
- Wireless Networks, Encryption and Threats
- Wireless Hacking Methodology
- Wi-Fi Encryption Cracking
- WEP/WPA/WPA2 Cracking Tools
- Bluetooth Hacking
- Bluetooth Threats
- Wi-Fi Security Auditing Tools
- Bluetooth Security Tools

Module 17: Hacking Mobile Platforms

- Mobile Platform Attack Vectors
- OWASP Top 10 Mobile Risks
- App Sandboxing
- SMS Phishing Attack (SMiShing)
- Android Rooting
- Hacking Android Devices
- Android Security Tools
- Jailbreaking iOS
- Hacking iOS Devices
- iOS Device Security Tools
- Mobile Device Management (MDM)
- OWASP Top 10 Mobile Controls
- Mobile Security Tools

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

Course Topics *Continued*

Module 18: Internet of Things (IoT) and Operational Technology (OT) Hacking

- IoT Architecture
- IoT Communication Models
- OWASP Top 10 IoT Threats
- IoT Vulnerabilities
- IoT Hacking Methodology
- IoT Hacking Tools
- IoT Security Tools
- IT/OT Convergence (IIOT)
- ICS/SCADA
- OT Vulnerabilities
- OT Attacks
- OT Hacking Methodology
- OT Hacking Tools
- OT Security Tools

Module 19: Cloud Computing

- Cloud Computing
- Types of Cloud Computing Services
- Cloud Deployment Models
- Fog and Edge Computing
- Cloud Service Providers
- Container
- Docker
- Kubernetes
- Serverless Computing
- OWASP Top 10 Cloud Security Risks
- Container and Kubernetes Vulnerabilities
- Cloud Attacks
- Cloud Hacking
- Cloud Network Security
- Cloud Security Controls
- Cloud Security Tools

Module 20: Cryptography

- Cryptography
- Encryption Algorithms
- MD5 and MD6 Hash Calculators
- Cryptography Tools
- Public Key Infrastructure (PKI)
- Email Encryption
- Disk Encryption
- Cryptanalysis
- Cryptography Attacks
- Key Stretching

LABS INCLUDED