EC-Council CEH – Certified Ethical Hacker
Course Version: C | EH v12

EC-Council

What is C|EH v12?

The Certified Ethical Hacker (CEH) Certification is a professional certification achieved through the EC-Council (International Council of E-Commerce Consultants) that develops modern cyber security skills as they relate to protecting virtual environments. The objective of the ethical hacker is to enable organizations to establish preventative measures against malevolent cyber-attacks by probing the system themselves for security flaws while staying within legal confines. 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

LEARNERSONE
Learning is a Safari

Course Breakdown

Domain 1	Introduction to Ethical Hacking	Domain 11	Session Hijacking
Domain 2	Footprinting and Reconnaissance	Domain 12	Evading IDS, Firewalls, and Honeypots
Domain 3	Scanning Networks	Domain 13	Hacking Web Servers
Domain 4	Enumeration	Domain 14	Hacking Web Applications
Domain 5	Vulnerability Analysis	Domain 15	SQL Injection
Domain 6	System Hacking	Domain 16	Hacking Wireless Networks
Domain 7	Malware Threats	Domain 17	Hacking Mobile Platforms
Domain 8	Sniffing	Domain 18	IoT Hacking
Domain 9	Social Engineering	Domain 19	Cloud Computing
Domain 10	Denial-of-Service	Domain 20	Cryptography

https://learnersone.com
(240) 930-4053

Program **Overview:**

LearnersOne's CEH certification training course provides you with the hands-on training required to master the techniques hackers use to penetrate network systems, helping you fortify your system against it. This ethical hacking course is aligned with the latest version of CEH (v12) by the EC-Council and adequately prepares you to increase your blue team skills.

Program **Features:**

- 40 hours of instructor-led training
- Accredited training partner of EC-Council
- Six months free access to CEH v12 iLabs
- Study material by EC-Council (e-kit)
- 20 current security domains
- Covers 340 attack technologies
- Exam pass guarantee (For the US only)

Delivery **Mode:**

Blended Learning

Prerequisites:

There is no specific eligibility criteria for Certified Ethical Hacker (CEH) training and certification, but we recommend a basic knowledge of TCP/IP.

Target **Audience:**

- Network security officers and practitioners
- Site administrators
- IS/IT specialist, analyst, or manager
- IS/IT auditor or consultant
- IT operations manager
- IT security specialist, analyst, manager, architect, or administrator
- IT security officer, auditor, or engineer
- Network specialist, analyst, manager, architect, consultant, or administrator
- Technical support engineer
- Senior systems engineer
- Systems analyst or administrator

Key Learning **Outcomes:**

This ethical hacking course will help you:

- Grasp the step-by-step methodology and tactics that hackers use to penetrate network systems
- Understand the finer nuances of trojans, backdoors, and countermeasures
- Get a better understanding of IDS, firewalls, honeypots, and wireless hacking
- Master advanced hacking concepts, including mobile device and smartphone hacking, writing virus codes, exploit writing and reverse engineering, and corporate espionage
- Gain expertise on advanced concepts such as advanced network packet analysis, securing IIS and Apache web servers, Windows system administration using Powershell, and hacking SQL and Oracle databases
- Cover the latest developments in mobile and web technologies, including Android, iOS, BlackBerry, Windows Phone, and HTML 5
- Learn advanced log management for information assurance and manage information security with more clarity

Certification **Alignment:**

Our Certified Ethical Hacker course is accredited by the EC-Council. We are the registered training provider for this course.

Certification Details and **Criteria:**

Certification Details -

To become CEH certified, you must pass the CEH examination after either attending CEH training at an accredited training center like LearnersOne or through self-study. If you choose self-study, you must fill out an application and submit proof of at least two years of experience in the network security domain. The purpose of the CEH credential is to:

- Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures
- Inform the public that credentialed individuals meet or exceed the minimum standards
- Reinforce ethical hacking as a unique and self-regulating profession

Course **Curriculum:**

Module 01 - Introduction to Ethical Hacking

- Lesson 01 - Information Security Overview
- Lesson 02 - Information Security Threats and Attack Vectors
- Lesson 06 - Penetration Testing Concepts
- Lesson 03 - Hacking Concepts
- Lesson 04 - Ethical Hacking Concepts
- Lesson 05 - Information Security Controls
- Lesson 07 - Information Security Laws and Standards

Module 02 - Footprinting and Reconnaissance

- Lesson 01 - Footprinting Concepts
- Lesson 02 - Footprinting through Search Engines
- Lesson 03 - Footprinting through Web Services
- Lesson 04 - Footprinting through Social Networking Sites
- Lesson 05 - Website Footprinting
- Lesson 06 - Email Footprinting
- Lesson 07 - Competitive Intelligence
- Lesson 08 - Whois Footprinting
- Lesson 09 - DNS Footprinting
- Lesson 10- Network Footprinting
- Lesson 11- Footprinting through Social Engineering
- Lesson 12 - Footprinting Tools
- Lesson 13 - Countermeasures
- Lesson 14 - Footprinting Pen Testing

Module 03 - Scanning Networks

- Lesson 01 - Network Scanning Concepts
- Lesson 02 - Scanning Tools

- Lesson 03 - Scanning Techniques
- Lesson 04 - Scanning Beyond IDS and Firewall
- Lesson 05 - Banner Grabbing
- Lesson 06 - Draw Network Diagrams
- Lesson 07 - Scanning Pen Testing

Module 04 - Enumeration

- Lesson 01 - Enumeration Concepts
- Lesson 02 - NetBIOS Enumeration
- Lesson 03 - SNMP Enumeration
- Lesson 04 - LDAP Enumeration
- Lesson 05 - NTP Enumeration
- Lesson 06 - SMTP Enumeration and DNS Enumeration
- Lesson 07 - Enumeration Countermeasures
- Lesson 08 - Other Enumeration Techniques
- Lesson 09 - Enumeration Pen Testing

Module 05 - Vulnerability Analysis

- Lesson 01 - Vulnerability Assessment Concepts
- Lesson 02 - Vulnerability Assessment Solutions
- Lesson 03 - Vulnerability Scoring Systems
- Lesson 04 - Vulnerability Assessment Tools
- Lesson 05 - Vulnerability Assessment Reports

Module 06 - System Hacking

- Lesson 01 - System Hacking Concepts
- Lesson 02 - Cracking Passwords
- Lesson 03 - Escalating Privileges
- Lesson 04 - Executing Applications
- Lesson 05 - Hiding Files
- Lesson 06 - Covering Tracks
- Lesson 07 - Penetration Testing

Module 07 - Malware Threats

- Lesson 01 - Malware Concepts
- Lesson 02 - Trojan Concepts
- Lesson 03 - Virus and Worm Concepts
- Lesson 04 - Malware Analysis
- Lesson 05- Countermeasures
- Lesson 06- Anti-Malware Software
- Lesson 07- Malware Penetration Testing

Module 08 - Sniffing

- Lesson 01- Sniffing Concepts
- Lesson 02- Sniffing Technique: MAC Attacks
- Lesson 03- Sniffing Technique: DHCP Attacks
- Lesson 04- Sniffing Technique: ARP Poisoning
- Lesson 05- Sniffing Technique: Spoofing Attacks
- Lesson 06- Sniffing Technique: DNS Poisoning
- Lesson 07- Sniffing Tools
- Lesson 08- Countermeasures
- Lesson 09- Sniffing Detection Techniques
- Lesson 10- Sniffing Pen Testing

Module 09- Social Engineering

- Lesson 01 - Social Engineering Concepts
- Lesson 02 - Social Engineering Techniques
- Lesson 03- Insider Threats
- Lesson 04 - Impersonation on Social Networking Sites
- Lesson 05 - Identity Theft
- Lesson 06 - Countermeasures
- Lesson 07 - Social Engineering Penetration Testing

Module 10- Denial-of-Service

- Lesson 01 - DoS/DDoS Concepts
- Lesson 02 - DoS/DDoS Attack Techniques
- Lesson 03 - Botnets
- Lesson 04 - DDoS Case Study
- Lesson 05 - DoS/DDoS Attack Tools
- Lesson 06 - Countermeasures
- Lesson 07 - DoS/DDoS Protection Tools
- Lesson 08 - DoS/DDoS Attack Penetration Testing

Module 11- Session Hijacking

- Lesson 01- Session Hijacking Concepts
- Lesson 02- Application-Level Session Hijacking
- Lesson 03- Network Level Session Hijacking
- Lesson 04- Session Hijacking Tools
- Lesson 05- Countermeasures
- Lesson 06- Penetration Testing

Module 12 - Evading IDS, Firewalls, and Honeypots

- Lesson 01- IDS, Firewall, and Honeypot Concepts
- Lesson 02- IDS, Firewall, and Honeypot Solutions
- Lesson 03- Evading IDS
- Lesson 04- Evading Firewalls
- Lesson 05- IDS/Firewall Evading Tools
- Lesson 06- Detecting Honeypots
- Lesson 07- IDS/Firewall Evasion Countermeasures
- Lesson 08- Penetration Testing

Module 13- Hacking Web Servers

- Lesson 01- Web Server Concepts
- Lesson 02- Web Server Attacks
- Lesson 03- Web Server Attack Methodology

Lesson 04- Web Server Attack Tools

- Lesson 05- Countermeasures
- Lesson 06- Patch Management
- Lesson 07- Web Server Security Tools
- Lesson 08- Web Server Pen Testing

Module 14- Hacking Web Applications

- Lesson 01 - Web App Concepts
- Lesson 02 - Web App Threats
- Lesson 03 - Hacking Methodology
- Lesson 04 - Web Application Hacking Tools
- Lesson 05 - Countermeasures
- Lesson 06 - Web App Security Testing
- Tools Lesson 07 - Web App Pen Testing

Module 15- SQL Injection

- Lesson 01 - SQL Injection Concepts
- Lesson 02 - Types of SQL Injection
- Lesson 03 - SQL Injection Methodology
- Lesson 04 - SQL Injection Tools
- Lesson 05 - Evasion Techniques
- Lesson 06 – Countermeasures

Module 16- Hacking Wireless Networks

- Lesson 01 - Wireless Concepts
- Lesson 02 - Wireless Encryption
- Lesson 03 - Wireless Threats
- Lesson 04 - Wireless Hacking Methodology
- Lesson 05 - Wireless Hacking Tools
- Lesson 06 - Bluetooth Hacking
- Lesson 07 - Countermeasures

Lesson 08 - Wireless Security Tools

Lesson 09 - Wi-Fi Pen Testing

Module 17- Hacking Mobile Platforms

- Lesson 01- Mobile Platform Attack Vectors
- Lesson 02- Hacking Android OS
- Lesson 03- Hacking iOS
- Lesson 04- Mobile Spyware
- Lesson 05- Mobile Device Management
- Lesson 06- Mobile Security Guidelines and Tools
- Lesson 07- Mobile Pen Testing

Module 18- IoT Hacking

- Lesson 01- IoT Concepts
- Lesson 02- IoT Attacks
- Lesson 03- IoT Hacking Methodology
- Lesson 04- IoT Hacking Tools
- Lesson 05- Countermeasures
- Lesson 06- IoT Pen Testing

Module 19- Cloud Computing

- Lesson 01 - Cloud Computing Concepts
- Lesson 02 - Cloud Computing Threats
- Lesson 03 - Cloud Computing Attacks
- Lesson 04 - Cloud Security
- Lesson 05 - Cloud Security Tools
- Lesson 06 - Cloud Penetration Testing

Module 20- Cryptography

- Lesson 01- Cryptography Concepts
- Lesson 02- Encryption Algorithms
- Lesson 03- Cryptography Tools

- Lesson 04- Public Key Infrastructure (PKI)
- Lesson 05- Email Encryption
- Lesson 06- Disk Encryption
- Lesson 07- Cryptanalysis
- Lesson 08- Countermeasures