ExecuTrain
Querétaro

C|EH v13

BECOME A CERTIFIED ETHICAL HACKER

Powered by AI Capabilities

LEARN | CERTIFY | ENGAGE | COMPETE

EC-Council C|EH v13 Certified Ethical Hacker

ExecuTrain
Líder en capacitación empresarial
Querétaro

Certified Ethical Hacker

C|EH v13

40 Hrs

Build Your Career with the Most In-Demand Ethical Hacking Certification

Ranked 1st in Ethical Hacking Certifications by ZDNet

Ranked in the List of Top 10 Cybersecurity Certifications

Ranked 4th Among the Top 50 Leading Cybersecurity Certifications

01 The World's #1 Ethical Hacking Certification for 20+ years

01 EC-Council Introduces the Industry's First AI Cybersecurity Courses

12 C|EH Ranks 12th among the Top 75 Highest-Paying IT Certifications in the US and Globally

97% Stated That the Skills They Acquired in CEH Helped Safeguard Their Organizations

95% Chose C|EH for Career Growth

92% of Hiring Managers Prefer Candidates with the C|EH for Jobs That Require Ethical Hacking Skills

45+ Cybersecurity Job Roles Are Mapped to the C|EH Certification in 2024, Compared to 20+ Roles in 2022

1 in every 2 Professionals Received Promotions After Completing the C|EH

C|EH is the only Globally In-Demand Ethical Hacking Certification that covers Core Domains of Cybersecurity and has Global Recognition and Accreditations while offering a Higher Employability Rate

What's New in The CEH v13

The C|EH v13 not only provides extensive hands-on coverage but also integrates AI into all five phases of ethical hacking:

Get C|EH Trained from Anywhere with our World-Class Instructors

1. Live-Online
2. Self-Paced Video Lectures
3. In-Person training
4. Masterclass

The AI Powered Certified Ethical Hacker

ExecuTrain Querétaro

Master AI to Automate Ethical Hacking Tasks, to hack and defend against AI systems,

and boost your task efficiency by 40% in your job role.

Develop a Hacker's Mindset: Master the 5 Phases of Ethical Hacking and Gain AI Skills to Automate Them

1. Reconnaissance

| Learn to gather essential information about your target

2. Vulnerability Scanning

| Gain the ability to identify weaknesses in the target system

3. Gaining Access

| Learn how to actively exploit identified vulnerabilities

4. Maintaining Access

| Develop skills to maintain continued access to the target systems

5. Clearing Tracks

| Master the art of erasing any trace of your activities

Learn AI Tools:

- ShellGPT
- ChatGPT
- FraudGPT
- WormGPT
- DeepExploit
- Nebula
- Veed.io

And many more!

ExecuTrain Querétaro

Learn

Learn ethical hacking with the revolutionary C|EH v13—a game-changer for aspiring ethical hackers.

With 20 cutting-edge modules, you'll gain the core skills needed to dominate the cybersecurity landscape. C|EH isn't just keeping pace—it's leading the charge, evolving with the latest operating systems, exploits, tools, and hacking techniques to ensure you're always ahead of the curve.

Dive deep into the future of cybersecurity with training that integrates AI into all five phases of ethical hacking, reconnaissance and scanning to gaining access, maintaining access, and covering tracks. You'll harness the power of AI to supercharge your hacking techniques and disrupt AI systems—giving you 10x efficiency in your cybersecurity role.

CEH v13 isn't just a certification; it's a fully immersive experience. CEH combines comprehensive knowledge-based training with immersive hands-on labs to ensure a well-rounded learning experience. You'll engage with live targets, tools, and vulnerable systems in a controlled environment, building real-world skills that empower you to confidently apply your expertise in any scenario. Get ready to transform the way you hack and protect the digital world!

Course Outline

Get the AI edge with 20 Power-packed Modules of the CEH v13

Learn	Course Outline
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 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 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.

Learn	Course Outline
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 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.

Hands-On Learning Labs

With 221 hands-on labs in our cutting-edge cyber range, you'll practice every skill on live machines and real-world vulnerabilities. Armed with over 4,000 powerful hacking tools and a range of operating systems, you'll gain unrivaled, practical expertise with the most widely used security tools, current vulnerabilities, and industry-standard operating systems.

This revolutionary environment brings the industry's top security tools and the latest vulnerabilities to your fingertips, all in a web-accessible platform. No matter where you are, you can dive into the real-world experience and emerge as a force to be reckoned with in cybersecurity.

Lab Environment

Cloud-Based Cyber Range

What's Covered

100% virtualization for a complete learning experience

Full access to pre-configured targets, networks, and the attack tools necessary to exploit them:

Pre-configured vulnerable websites

Vulnerable, unpatched operating systems

Fully networked environments

4000+ hacking tools and so much more!

Wide range of target platforms to hone your skills

550 attack techniques covered

Objective-oriented flags for critical thinking and applied knowledge assessment

Cloud-based cyber range