EC-Council – Certified Ethical Hacker (CEHv12 EN)

EC-Council – Certified Ethical Hacker (CEH version 12)

The World’s No. 1 Ethical Hacking Certification for 20 Years

About this Course

What is C|EH® v12?
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, handson 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.

Who is a Certified Ethical Hacker? A Certified Ethical Hacker is a specialist typically working in a red team environment, focused on attacking computer systems and gaining access to networks, applications, databases, and other critical data on secured systems. 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.

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information
security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it
is recognized as a standard within the information security community. CEH v12 continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used
by hackers and information security professionals today. The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: “To beat a hacker, you need to think like a hacker

CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so that you will be better positioned to set up your security infrastructure and defend future attacks. Understanding system weaknesses and vulnerabilities help organizations strengthen their

system security controls to minimize the risk of an incident. CEH was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure. In its 11th version, CEH continues to evolve with the latest operating systems, tools, tactics, exploits,
and technologies. Here are some critical updates of CEH v12:

20 Modules That Help You Master the Foundations of Ethical Hacking and Prepare to Take the C|EH Certification Exam

1. C|EHv12 Learn

The C|EH v12 training program curates 20 modules covering a wide variety of technologies, tactics, and procedures providing prospective Ethical Hackers with the core knowledge needed to thrive in the cyber profession. Concepts covered in the training program are balanced 50/50 with knowledge and hands-on application through our Cyber range.

Every tactic discussed in training is backed by step-by-step labs conducting in a live virtualized environment with live targets, live tools, and vulnerable systems. WITH OVER 220 LABS, AND our Lab technology, you will have comprehensive hands-on practice to learn and apply the knowledge you attain.

2. C|EHv12 Certify

The Certified Ethical Hacker Credential is the most trusted certification across the globe, and is the baseline measurement of ones grasp on the concepts in ethical hacking and security testing. As an ANSI

17024 accredited examination, the 125 question, 4-hour proctored exam is recognized across the globe as the original, and most trusted tactical cyber security certification for ethical hackers.

Each of the Certification Domains are carefully vetted through industry practitioners ensuring the certification maps to current industry requirements. This exam undergoes regular psychometric evaluation and tuning to ensure a fair and accurate measure of the candidate’s knowledge in the Ethical Hacking domains.

C|EH MASTER? After completing the C|EH exam, you also have the opportunity to elevate your credentials. You can take the practical exam that consists of 20 practical challenges in a 6-hour period. Just envision your title as a C|EH Master, this credential will set you apart from you fellow peers.

3. C|EHv12 Engage

New to C|EH v12, students will embark on their first emulated ethical hacking engagement. This 4-phase engagement requires the student to think critically and apply the knowledge and skills gained in the course. Learners will perform and capture a series of flags in each phase demonstrating the live application of skills and abilities in a consequence free environment, in EC-Council’s new Cyber Range.

4. C|EHv12 Compete

The compete phase, new to C|EH v12, the C|EH Global Challenges run every month providing Capture-The-Flag style competitions exposing Certified Ethical Hackers to a variety of modern technologies and platforms from Web Applications, OT, IoT, SCADA and ICS systems, to Cloud and Hybrid environments. Our Compete structure allows C|EH’s to fight their way to the top

of the leader board each month in these 4-hour curated CTF's.

Objective based flags are designed around the Ethical Hacking process keeping the C|EH's skills current, assessing their critical thinking abilities and covering the latest vulnerabilities and exploits as they are discovered. The capture-the-flag competitions are hosted 100% online in EC-Council's Cyber Range.

Candidates race the clock in scenario-based engagements against fully developed Network and application environments with operating systems, real networks, real tools, and real vulnerabilities.

Key Updates to the C|EH v12

Content Updates

1. New Learning Framework: 1. Learn 2. Certify 3. Engage 4. Compete
2. Compete: New challenges every month!
3. 100% compliance with the NICE 2.0 Framework
4. Based on comprehensive industry-wide job task analysis
5. Hands-on Learning Labs
6. Practice Range
7. Global C|EH community competitions
8. Cheat sheet
9. Coverage of the latest malware
10. Lab-intensive program (every learning objective is demonstrated using labs)
11. Hands-on program (50% of training time is dedicated to labs)
12. Lab environments that simulate real-time environments
13. Covers the latest hacking tools (based on Windows, macOS, and Linux)
14. Latest OS covered and a patched testing environment
15. Updated versions of tool screenshots, tool listing

slides, and countermeasure slides

Technology Updates

1. MITRE ATT&CK framework
2. Diamond model of intrusion analysis
3. Techniques for establishing persistence
4. Evading NAC and endpoint security
5. Fog computing
6. Edge computing
7. Grid computing

Course Goals

What You Will Learn ?
Introduction to Ethical Hacking
Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.
Foot Printing and Reconnaissance
Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.
Scanning Networks
Learn different network scanning techniques and countermeasures.
Enumeration
Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, and associated countermeasures.
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.System Hacking
Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used

to discover system and network vulnerabilities.

Malware Threats

Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures.

Sniffing

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Social Engineering

Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

Denial-of-Service

Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Session Hijacking

Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Evading IDS, Firewalls, and Honeypots

Get introduced to firewall, intrusion detection system (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Hacking Web Servers

Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Hacking Web Applications

Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures

SQL Injection

Learn about SQL injection attacks, evasion techniques, and SQL injection countermeasures.

Hacking Wireless Networks

Understand different types of wireless technologies, including

encryption, threats, hacking methodologies, hacking tools, Wi-Fi sedcurity tools, and countermeasures.

Hacking Mobile Platforms

Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

IoT Hacking

Learn different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures.

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.

Cryptography

Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

Course Format

[table id=1 /]

Course Language Option

[table id=2 /]

Student Resources

Digital Asset available for lifetime after the training.

Lab Environment

Dedicated Lab Environment

With over 220 hands-on labs conducted in our cyber range environment, you will have the opportunity to practice every learning objective on live machines and vulnerable targets in the course. Pre-loaded with over 3,500 hacking tools and various operating systems, you will gain unprecedented exposure and hands-on experience with the most common security tools,
latest vulnerabilities, and widely used operating systems in the industry. Our range is web accessible, making it easier for you to learn and practice from anywhere.

At Course Completion

[table id=3 /]

Course Duration

- 5 working days (09:00 – 17:00 / 9:00 am – 5:00 pm) UTC +2 (contact us for another Time Zone)

or

- **40 learning hours after hours (2 weeks, classes are held 2 times a week in one of the following options):**
- Sat. and Sun. 10:00 – 14:00 or 14:00 – 18:00 or 18:00 – 22:00
- Mon. and Wed. 19:00 – 23:00
- Tue. or Thu. 19:00 – 23:00

Payments

Course Schedules

[tribe_events_list category="ceh"]

If you dont see a date, contact us.

All classes are confirmed individually after enrollment.

All EC-Council Course Schedules

[tribe_events_list category="ec-council"]

CEHv12 Brochure.cleaned