



The All-New

**C | EH<sup>®</sup> v12**  
Certified Ethical Hacker

**1 LEARN**

**2 CERTIFY**

**3 ENGAGE**

**4 COMPETE**

Attain the World's No.1 Credential in  
Ethical Hacking

Build your career with the most in-demand cybersecurity certification in the world:

# THE CERTIFIED ETHICAL HACKER

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



**Ranked #1**  
In Ethical Hacking  
Certifications by ZDNet



**Ranked as a Top 10**  
Cybersecurity Certification



**C|EH® Ranks 4<sup>th</sup>**  
Among Top 50 Leading  
Cybersecurity Certifications

## 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.





## 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, 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 C|EH v12 also equips aspiring cybersecurity professionals 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.

# What's New in the C|EH® v12

## LEARN | CERTIFY | ENGAGE | COMPETE

The C|EH® v12 is a specialized and one-of-a-kind training program to teach you everything you need to know about ethical hacking with hands-on training, labs, assessment, a mock engagement (practice), and global hacking competition. Stay on top of the game with the most in-demand skills required to succeed in the field of cybersecurity.

**Master ethical hacking skills that go beyond the certification.**

**1** LEARN




Gain Skills

**2** CERTIFY



Gain Recognition

**3** ENGAGE



Gain Experience

**4** COMPETE



Gain Respect

The new learning framework covers not only a comprehensive training program to prepare you for the certification exam but also the industry's most robust, in-depth, hands-on lab and practice range experience.

# Enter the Hackerverse™ With the C|EH® v12

## Enhance Your Ethical Hacking Career

---

### 1 LEARN

- 5 days of training
- 20 modules
- 3000+ pages of student manual
- 1900+ pages of lab manual
- Over 200 hands-on labs with competition flags
- Over 3,500 hacking tools
  - Learn how to hack multiple operating systems (Windows 11, Windows servers, Linux, Ubuntu, Android)
- MITRE Attack Framework
- Diamond model of intrusion analysis
- Techniques for establishing persistence
- Evading NAC and endpoint security
- Understand Fog, Edge, and Grid Computing Model

### 3 ENGAGE

- Conduct a real-world ethical hacking assignment
- Apply the 5 phases
  - Reconnaissance
  - Scanning
  - Gaining Access
  - Maintaining Access
  - Covering Your Tracks

### 2 CERTIFY

#### C|EH® ANSI

- 125 Multiple-Choice Questions
- 4 hours

#### C|EH® Practical

- 6-hour Practical Exam
- 20 Scenario-Based Questions

### 4 COMPETE

- New challenges every month
- 4-hour competition
- Compete with your peers all over the world
- Hack your way to the top of the leaderboard
- Gain recognition
- Challenges include:
  - OWASP Top 10 Web Application Threat Vectors
  - Ransomware/Malware Analysis
  - Outdated/Unpatched Software
  - System Hacking and Privilege Escalation
  - Web Application Hacking and Pen Testing
  - Cloud Attack/Hacking
  - and many more...

# LEARN

The C|EH® v12 training program includes 20 modules covering various technologies, tactics, and procedures, providing prospective ethical hackers with the core knowledge needed to thrive in cybersecurity. Delivered through a carefully curated training plan that typically spans five days, the 12th version of the C|EH® continues to evolve to keep up with the latest OS, exploits, tools, and techniques. The concepts covered in the training program are split 50/50 between knowledge-based training and hands-on application through our cyber range. Every tactic discussed in training is backed by step-by-step labs conducted in a virtualized environment with live targets, live tools, and vulnerable systems. Through our lab technology, every participant will have comprehensive hands-on practice to learn and apply their knowledge.”

20

REFRESHED  
MODULES

3000+

PAGES OF  
STUDENT MANUAL

## Course Outline

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

- |                  |   |
|------------------|---|
| <b>Module 01</b> | <b>Introduction to Ethical Hacking</b><br>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. |
| <b>Module 02</b> | <b>Foot Printing and Reconnaissance</b><br>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.                              |
| <b>Module 03</b> | <b>Scanning Networks</b><br>Learn different network scanning techniques and countermeasures.  |
| <b>Module 04</b> | <b>Enumeration</b><br>Learn various enumeration techniques, such as 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.
- 
- Module 06** | **System Hacking**  
Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.
- 
- Module 07** | **Malware Threats**  
Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures.
- 
- Module 08** | **Sniffing**  
Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as 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, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.
- 
- Module 11** | **Session Hijacking**  
Understand 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**  
Get introduced to firewall, intrusion detection system (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 web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.
- 
- Module 15** | **SQL Injection**  
Learn about SQL injection attacks, evasion techniques, and SQL injection countermeasures.
- 
- Module 16** | **Hacking Wireless Networks**  
Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi security tools, and countermeasures.
- 
- Module 17** | **Hacking Mobile Platforms**  
Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.
- 
- Module 18** | **IoT Hacking**  
Learn different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures.
- 
- Module 19** | **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.
- 
- 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 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.

## What's Covered:

100% virtualization for a complete learning experience

Wide range of target platforms to hone your skills

After login, you will have 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
- 3,500+ hacking tools
- And much more!

519 attack techniques

Objective-oriented flags for critical thinking and applied knowledge assessment

Cloud-based cyber range



# 3 ENGAGE

The C|EH® v12 program helps you develop real-world experience in ethical hacking through the hands-on C|EH® practice environment. The C|EH® Engage equips you with the skills to prove that you have what it takes to be a great ethical hacker.

New to C|EH® v12, students will embark on their first emulated ethical hacking engagement. This 4-phase engagement requires students to think critically and test the knowledge and skills gained by capturing a series of flags in each phase, demonstrating the live application of skills and abilities in a consequence-free environment through EC-Council's new Cyber Range.

As you complete your training and hands-on labs, the C|EH® Engage lets you apply everything you have learned in a mock ethical hacking engagement. This 4-part security engagement gives you a real ethical hacking engagement experience from start to finish against an emulated organization. Using our capture-the-flag-style range, you will complete your engagement by answering "flag" questions as you progress.

## Your Mission

Whether this is your first engagement or you're honing your skills, get ready to test your ethical hacking knowledge like never before! Once you've practiced through the hands-on guided labs, it's time to apply your knowledge, take on the hacker persona, and find the vulnerabilities and weaknesses in ABCorg—all built in our C|EH® Engage (practice range).

## Target Organization Characteristics

ABC is a Nationwide IT/ITES organization	Realistic segmented networks	DMZs's and private subnets stretch across the infrastructure to support various business units	Various application servers and services support ABCDORG Operations
Real networks, real operating systems, and real applications	Private, dedicated access – no shared resources	Fully automated network deployment with EC-Council's Cyber Range	24x7 browser-based access

## Objectives:

Armed with your attack platform, Kali Linux OS, and a plethora of tools used by Ethical Hackers, you will embark on a 4-part engagement to assess ABCorg's security posture. Follow the process, practice your TTP and experience the real thing in a controlled environment with no consequences, just the ultimate learning experience to support your career as an Ethical Hacker! Each phase builds on the last as you progress through your ABCorg's engagement.

- Foot Printing & Reconnaissance
- Scanning
- Enumeration
- Vulnerability Analysis

### PHASE 1 Vulnerability Assessment

- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service

### PHASE 2 Gaining Access

- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- OT Hacking
- Cloud Computing
- Cryptography

### PHASE 4 Mobile, IoT, OT Exploitation

### PHASE 3 Perimeter and Web App Exploitation

- Session Hijacking
- Evading IDS
- Firewalls
- Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection

## Put Your Skills and Knowledge to the Test With the C|EH® Master

Once you have achieved the certification and completed your ethical hacking engagement, you are ready to challenge the proctored C|EH® practical assessment and become a C|EH® Master!

# 4 COMPETE

## Without a Stimulating Cyber Competition, There Can Be No Progress. Competitors Drive You to Be the Best You Can Be.

The C|EH® Global Challenges occur every month, providing capture-the-flag style competitions that give students exposure to various new technologies and platforms, from web applications, OT, IoT, SCADA, and ICS systems to cloud and hybrid environments. Our compete structure lets ethical hackers fight their way to the top of the leaderboard each month in these 4-hour curated CTFs. Objective-based flags are designed around the ethical hacking process, keeping skills current, testing critical thinking abilities, and covering the latest vulnerabilities and exploits as they are discovered. 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 real operating systems, real networks, tools, and vulnerabilities to practice, engage, compete, build, and hone their cyber skills against various new target organizations.

### The All-New C|EH® Global Challenges

Each month will present a different theme and challenge with Capture-The-Flag style competitions focusing on ethical hackers' core skills and abilities. Gain exposure to new tools, focus on new attack vectors, and try to exploit emerging vulnerabilities while gaining continuing education credits and keeping your skills and certifications current

### New Challenges Every Month!

Assignments	Skill Challenge
OWASP TOP 10	OWASP Top 10 Web Application Threat Vectors
MALWARE	Ransomware/Malware Analysis
SOFTWARE	Outdated/Unpatched Software
SYSTEM HACKING	System Hacking and Privilege Escalation
WEB APP HACKING	Web Application Hacking and Pen Testing
CLOUD COMPUTING	Cloud Attack/Hacking
SOCIAL ENGINEERING	Social Engineering/Phishing attacks
IoT AND OT	IoT Attack/Hacking
WIFI ATTACK	Wi-Fi Network Attack/Hacking
DOS/DDoS	DOS/DDoS Attack
MOBILE ATTACK	Mobile Attack/Hacking
SUPPLY CHAIN ATTACK	Supply Chain Cyber Attacks



## Compete Until Everyone Knows You

As an Ethical Hacker, you will battle your way to the top of the monthly Leaderboards as you race the clock in these 4-hour CTF challenges. Open all month long, the choice is yours as to when you compete, but show up ready! All you need is a connection, compete through your browser, we provide the attack platform, the targets, and all the tools, you bring the skills to win!

## Prerequisites

All you need is a connection, and you can compete through your browser. We provide the attack platform, the targets, and all the required tools. You bring the skills to win!



## Compete Example Preview of Upcoming Challenges

**Topic:**  
Ransomware/  
Malware Analysis

**Brief:** You have been called in by a reputed MNC hit with malware recently. This has locked up their services and managed to infect a slew of customers that were also using their solution. The incident response team managed to extract some of the code, and now your job is to reverse engineer the malware and identify the encryption algorithms used, as well as identify any trace of command-and-control servers that may be helpful to law enforcement agencies.

**Topic:**  
Application  
Hardening

**Brief:** Your employer, a large financial institution, has suffered a breach where hackers were able to inject code into a web application that exposed sensitive customer data. Your company has faced tremendous scrutiny from the public and had to pay fines to its regulators. You have performed a series of manual and automated tests against the web application to identify weaknesses and provide recommended countermeasures to the app sec team.

## Key Updates of C|EH® v12

### Features:

1. New Learning Methodology: Learn – Certify – Engage – Compete
2. Compete: new challenges every month to test your job-ready skills!
3. 100% Compliance to NICE 2.0 Framework
4. Based on a 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 (More than 50% of training time is dedicated to labs)
12. Lab environment simulates a real-time environment(Lab setup simulates real-life networks and platforms)
13. Covers the latest hacking tools (Based on Windows, macOS, and Linux)
14. Latest OS covered and a patched testing environment
15. All the tool screenshots are replaced with the latest version
16. All the tool listing slides are updated with the latest tools
17. All the countermeasure slides are updated

### Technology Updates:

1. MITRE ATTACK 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

## Common Job Roles for C|EH

- Mid-Level Information Security Auditor
- Cybersecurity Auditor
- Security Administrator
- IT Security Administrator
- Cyber Defense Analyst
- Vulnerability Assessment Analyst
- Warning Analyst
- Information Security Analyst 1
- Security Analyst L1
- Infosec Security Administrator
- Cybersecurity Analyst level 1, level 2, & level 3
- Network Security Engineer
- SOC Security Analyst
- Security Analyst
- Network Engineer
- Senior Security Consultant
- Information Security Manager
- Senior SOC Analyst
- Solution Architect
- Cybersecurity Consultant



# Discover Why C|EH® Is Trusted by Organizations Around the World!

For 7 years, SBComputer's Ethical Hacking programs have empowered many professionals in Nepal to exercise their training and expertise to combat cyberattacks. SBComputer celebrates those individuals who have excelled, achieved, and fostered a spirit of leadership among their colleagues and peers within the cyber community.

**97%**

**Rated the program topics as directly relevant to current real-world threats.**

**63%**

**Reported a direct pay raise or promotion after attaining their C|EH® certification.**

**95%**

**Responded being able to improve organizational security after completing the program.**





**WE DON'T JUST TEACH**  
**ETHICAL**  
**HACKING**  
**WE BUILD CYBER CAREERS**

**Attain the World's No.1 Credential in Ethical Hacking**