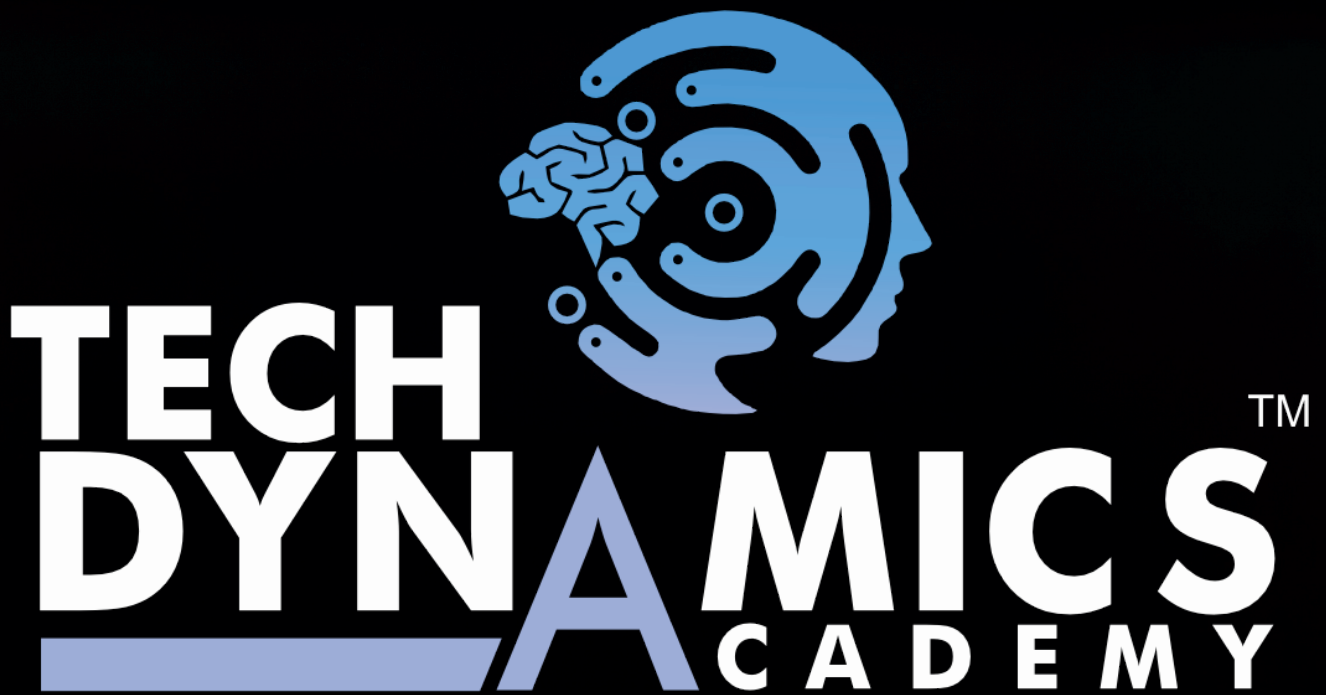




**EC-Council**  
Accredited  
Training Center



---


Information System & Cyber Security Academy

---

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**

---

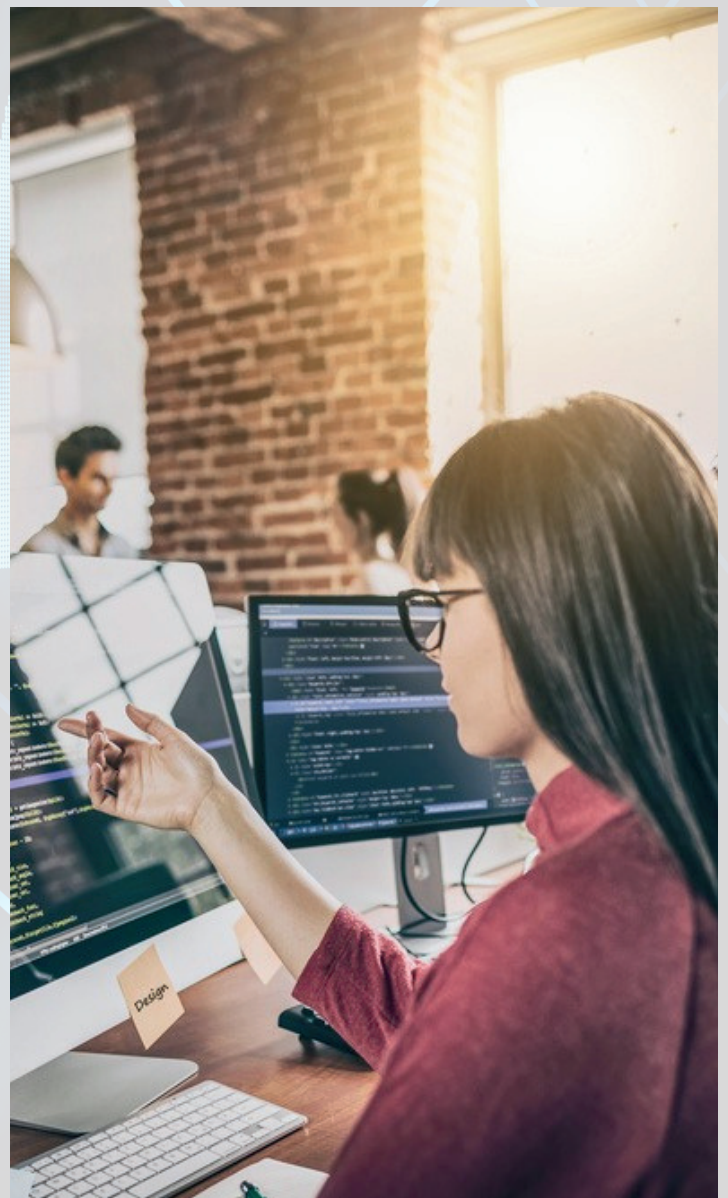
 **Ranked as a Top 10 Cybersecurity Certification**

---

 **C|EH® Ranks 4th 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.



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.

# Enter the Hackerverse™ With the C|EH® v12 Enhance Your Ethical Hacking Career

---

- 20 modules
- 3000+ pages of student manual
- 1900+ pages of lab manual
- 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

## **C|EH® ANSI**

- 125 Multiple-Choice Questions
- 4 hours



# 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

#### Module 01

##### 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.

#### Module 02

##### 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.

#### Module 03

##### Scanning Networks

Learn different network scanning techniques and countermeasures.

#### Module 04

##### Enumeration

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 and OT 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.

# 2 CERTIFY

## Prove Your Skills and Abilities With Online, Practical Examinations

The Certified Ethical Hacker® credential is trusted globally as the industry standard for evaluating one's understanding of ethical hacking and security testing. As an ANSI 17024 accredited examination, the 150-question, 4-hour proctored exam is recognized across the globe as the original and most trusted tactical cyber security certification for ethical hackers. 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 domain.



4 Hours  
Multiple-Choice Exam





## C|EH® v12

Upon completing the C|EH® program, consisting of the C|EH® have shown proficiency at a master level in the knowledge, skills, and abilities of ethical hacking with a total of 6 hours of testing to prove their competency. The top 10 performers in both C|EH® and C|EH® Practical exams are featured on the C|EH® Global Ethical Hacking Leader Board.

### The C|EH® Exam at a Glance

#### Exam Details

Number of Questions/Practical Challenges  
Test Duration  
Test Format  
Test Delivery  
Availability  
Exam Prefix  
Passing Score

#### C|EH® (MCQ Exam)

125  
4 Hours  
Multiple Choice Questions  
ECC EXAM, VUE  
-  
312-50 (ECC EXAM), 312-50 (VUE)  
Refer to  
<https://cert.eccouncil.org/faq.html>

- 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!

## Updated OS

<b>Windows 11</b>	<b>Windows Server</b>
<b>Parrot</b>	<b>2022 Windows</b>
<b>Security</b>	<b>Server 2019 Ubuntu</b>
<b>Android</b>	<b>Linux</b>

## Course Content

<b>3000+</b> Student Manual Pages	<b>1900+</b> Lab Manual Pages
<b>3500+</b> Hacking & Security Tools	<b>220</b> Hands-On Lab Practical
<b>519</b> Attack Techniques	<b>20</b> Refreshed Modules

## 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

# The NEW Vulnerability Assessment and Penetration Testing (VAPT) Track

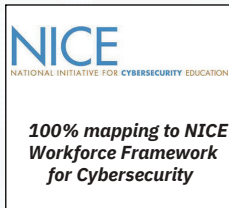
How to achieve C|EH and beyond!



*Trusted By*  
**FORTUNE 500 COMPANIES**

## C|EH® v12

### Recognition / Endorsement / Mapping



The national Initiative for Cybersecurity Education (NIC)



American National Standards Institute (ANSI)



Committee on National Security Systems (CNSS)



United States Department of Defense (DoD)



National Infocomm Competency Framework (NICF)



MSC



KOMLEK

## Why People Love C|EH®



“C|EH® certification made my CV outstanding compared to my peers, It has landed me an exciting role at EY.”

**Sidhant Gupta**, *Senior Security Consultant*, Hall of Fame nominee  
(EC-Council, How C|EH® Helped Me, 2021)

“What C|EH® gives you is a 360-degree view. So, what it leaves you with is a desire to learn more and more about an infinitely large subject where the individual matters little and the team matters a lot.”

**Lorenzo Neri**, *Security Specialist*, Hall of Fame finalist

“Becoming a C|EH® Master has given me the belief that I can progress further in the cybersecurity industry and inspired me to go further with my professional qualifications, hopefully enabling me to attain CREST accreditation.”

**Paul Mahoney**, *Network security and resilience manager* for a large ATM deployer,  
2021 Hall of Fame finalist

“I really like hands-on training, the labs are very intuitive. The program walks you through every step and breaks it down so you can understand it.”

**Richard Medlin**, *Pentester and Cybersecurity analyst*, an active-duty Marine and newly inducted member of the C|EH® Hall of Fame  
(EC-Council, An Active Duty Marine’s Journey, 2021)



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

For 20 years, EC-Council's cybersecurity programs have empowered cybersecurity professionals around the world to exercise their training and expertise to combat cyberattacks. The Hall of Fame 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.**

**Download the C|EH® Hall of Fame Report**

# About Us

Welcome to Tech Dynamics Academy, a trailblazer in the realm of cybersecurity education and consultancy. At Tech Dynamics, we understand that the digital landscape is constantly evolving, and so are the threats that accompany it. As a premier provider of system auditing and cybersecurity training, we stand at the forefront of safeguarding businesses and individuals from cyber vulnerabilities.

Our mission extends beyond mere protection; we are dedicated to fostering a culture of continuous learning and development. Tech Dynamics Academy is not just a training center; it's a hub where knowledge and innovation converge. Our team of industry experts brings real-world experience to the forefront, ensuring that our programs are practical, relevant, and aligned with the latest industry standards.

Whether you're an aspiring cybersecurity professional or an organization seeking to fortify your digital defenses, Tech Dynamics Academy provides tailored solutions to meet your needs. From hands-on training to strategic consultancy services, we empower our clients to navigate the complex landscape of cybersecurity with confidence.

Join us at Tech Dynamics Academy, where excellence meets education, and together, we shape a secure and resilient digital future. Elevate your skills, enhance your cybersecurity posture, and embark on a journey of continuous growth with Tech Dynamics Academy.

Learn more at [www.techdynamicsacademy.com](http://www.techdynamicsacademy.com)





Information System & Cyber Security Academy



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

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