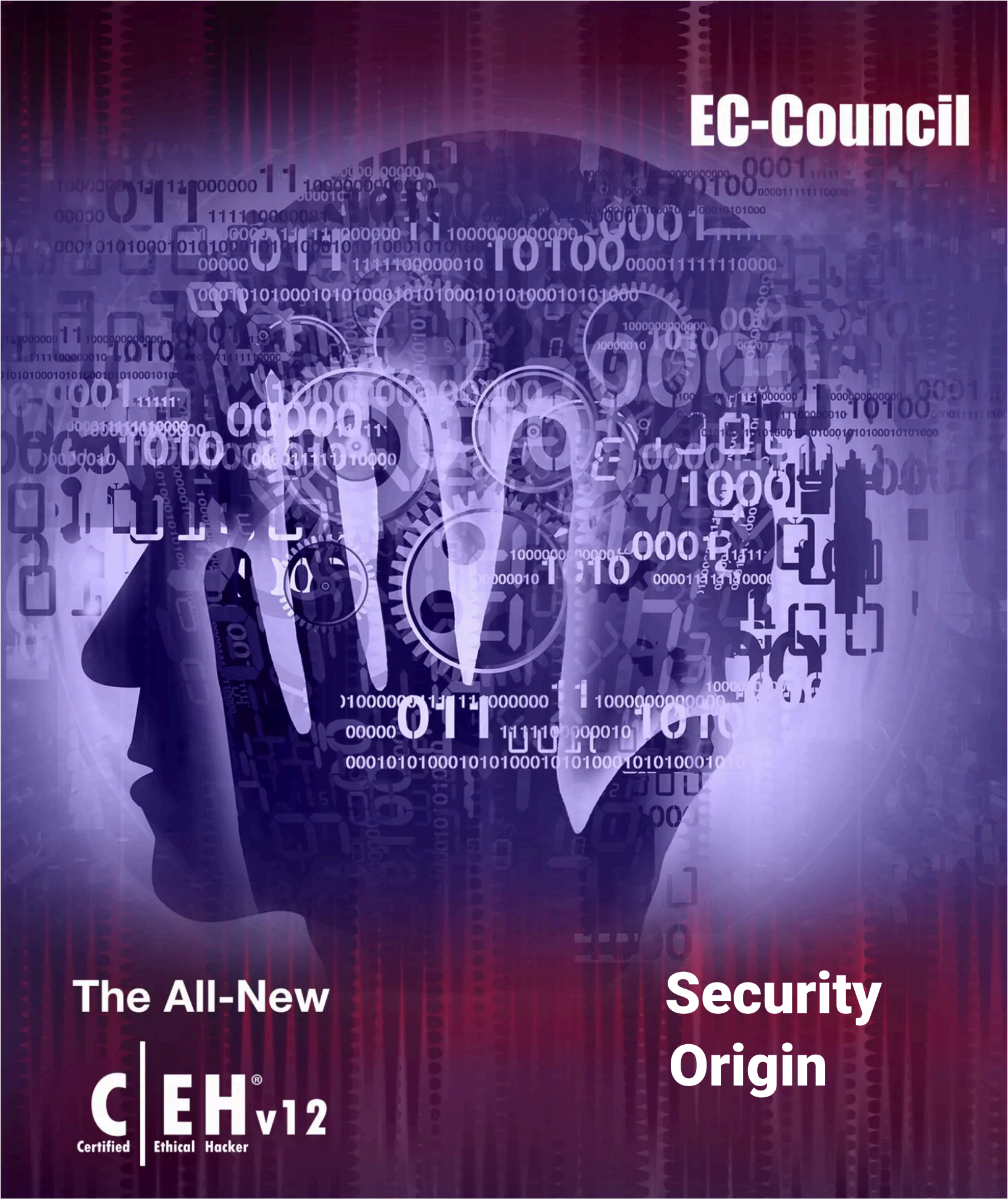
EC-Council



The All-New

C|EH® v12

Certified Ethical Hacker

Security Origin

Index:

Who is a Certified Ethical Hacker?

A Certified Ethical Hacker (C|EH) is a professional specializing in ethical hacking within a red team environment. Tasked with penetrating computer systems, they focus on accessing networks, applications, databases, and critical data on secured systems. C|EH practitioners possess expertise in attack strategies, creative attack vectors, and emulate the skills of malicious hackers. Crucially, they operate with explicit permission from system owners, ensuring confidentiality and distinctively differ from unauthorized actors. Bug bounty researchers, akin to expert ethical hackers, leverage their skills to identify vulnerabilities in systems.

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

Overview:

WHAT IS C|EH v12?

The Certified Ethical Hacker (C|EH) has stood the test of time, with a rich history spanning two decades. During this period, it has successfully molded hundreds of thousands of Certified Ethical Hackers who now hold positions in leading companies, military organizations, and governments globally.

Now in its 12th version, the Certified Ethical Hacker certification continues to deliver an extensive training experience. It combines comprehensive theoretical knowledge with practical, hands-on learning labs, engaging practice cyber ranges, certification assessments, cyber competitions, and avenues for continuous learning. This all-encompassing program is designed to provide aspiring cybersecurity professionals with a holistic understanding of the field.

The C|EH v12 is specifically crafted to empower individuals with the tactics, techniques, and procedures (TTPs) necessary to develop ethical hackers. These professionals are adept at identifying vulnerabilities in a diverse range of target systems, staying one step ahead of cybercriminals in safeguarding digital environments.

Why you should choose CEH v12:

- **Knowledge and Skills:**

The program covers a wide range of domains in cybersecurity, giving you the knowledge and skills you need to succeed in the field.

- **Think like a hacker:**

The CEH program is a vendor-neutral certification that covers a wide range of ethical hacking topics. By understanding how hackers think, you can better anticipate their attacks and develop defenses to protect your systems..

- **Return On Investment:**

The CEH program is a relatively small investment of your time and money, but it can lead to a lifetime of high-value returns.

- **Industry Recognition:**

The CEH certification is ANSI accredited, which means that it is recognized by employers around the world. Earning the CEH certification shows employers that you are qualified for the job and serious about your career in cybersecurity.

- **High Demand in the Job Market:**

CEH is a very well-known certification in the cybersecurity space with a high market share.Having this certification can increase your chances of landing a job in cybersecurity. A search for global job ads showed over 32,000 available jobs requesting candidates with a CEH Certification.

Overall, The CEH 12 certification offers a comprehensive cybersecurity curriculum, providing essential knowledge and skills for success. With a focus on ethical hacking and ANSI accreditation, this program ensures a valuable return on investment, recognized globally by employers and meeting the high demand for cybersecurity professionals in the job market.

Target Audience:

- **Ethical Hackers and Security Professionals:** Individuals involved or interested in ethical hacking, penetration testing, and cybersecurity roles aiming to enhance their skills and knowledge.
- **Security Officers and Auditors:** Security officers, auditors, and professionals responsible for ensuring the security of information systems and networks.
- **IT Professionals and Managers:** IT professionals, including managers, looking to deepen their understanding of ethical hacking principles for improved cybersecurity management.
- **Network and System Administrators:** Professionals overseeing network and system administration tasks, focused on maintaining secure computing environments.
- **Cyber Security Consultant:** Professionals who provides expert advice and solutions to organizations, advising on cybersecurity strategies and mitigating risks.
- **Anyone Pursuing a Career in Ethical Hacking or Cybersecurity:** Individuals aspiring to enter the field of ethical hacking and cybersecurity, seeking a foundational certification to establish their expertise

It's important to note that the CEH v12 certification is designed for professionals across a spectrum of roles who are interested in ethical hacking and cybersecurity. The certification provides a valuable skill set for those looking to defend against cyber threats and vulnerabilities.

Pre-requisites:

Basic idea of networking and its components. (Those who want to start from scratch, we will be providing you a comprehensive pathway training ensuring coverage of all the essential requirements to acquire optimal knowledge and skills from the CEH Program).

Exam Information:

The CEH exam challenges you with 125 multiple-choice questions over 4 hours. This knowledge-based test assesses your understanding of cybersecurity threats, how attackers exploit them, and the methods used to detect, prevent, and respond to such attacks.

Number of Questions: 125	Test Duration: 4 Hours
Test Format: Multiple Choice	Test Delivery: Remote proctored
Exam Prefix:	312-50 (ECC EXAM), 3123-50 (VUE)

Passing Score: ECC Council administers exams with various question banks featuring different difficulty levels. The passing scores can vary, ranging from 70% to 85%, contingent on the specific form of the exam undertaken.

Course Objectives:

Module 01: Introduction to Ethical Hacking.

-An overview of ethical hacking concepts, introducing participants to the principles and methodologies of ethical hacking.

Module 02: Footprinting and Reconnaissance

-Covers techniques for gathering information about a target system or network to identify potential vulnerabilities and entry points.

Module 03: Scanning Networks

-Explores network scanning methodologies to discover active hosts, services, and vulnerabilities within a network.

Module 04: Enumeration

-Focuses on extracting information about network resources, users, and shared services to gain insights for potential security threats.

Module 05: Vulnerability Analysis

-Examines methods for evaluating and analyzing system vulnerabilities to enhance the security posture.

Module 06: System Hacking

-Provides insights into techniques for unauthorized access, privilege escalation, and compromising system security.

Module 07: Malware Threats

-Addresses various types of malware, their characteristics, and methods for detection and mitigation.

Module 08: Sniffing

-Explores network sniffing techniques, understanding how attackers can capture and analyze data in transit.

Module 09: Social Engineering

-Discusses psychological manipulation techniques used by attackers to exploit human behavior and gain unauthorized access.

Module 10: Denial-of-Service

-Covers strategies and countermeasures against Denial-of-Service attacks, which aim to disrupt or disable network services.

Module 11: Session Hijacking

-Focuses on methods to take over an established session between two parties, potentially leading to unauthorized access.

Module 12: Evading IDS, Firewalls, and Honeypots

-Explores techniques to bypass intrusion detection systems, firewalls, and honeypots in order to evade detection.

Module 13: Hacking Web Servers

-Examines vulnerabilities and exploits associated with web servers, emphasizing securing web server infrastructure.

Module 14: Hacking Web Applications

-Addresses security issues related to web applications, covering common vulnerabilities and secure coding practices.

Module 15: SQL Injection

-Details SQL injection attacks, which involve manipulating databases through vulnerabilities in SQL queries.

Module 16: Hacking Wireless Networks

-Explores security challenges in wireless networks, covering common attacks and methods to secure wireless environments.

Module 17: Hacking Mobile Platforms

-Addresses security concerns in mobile platforms, covering vulnerabilities and safeguards for mobile devices.

Module 18: IOT and OT Hacking

-Examines the security risks associated with Internet of Things (IoT) and Operational Technology (OT) devices and systems.

Module 19: Cloud Computing

-Explores security considerations and best practices in cloud computing environments.

Module 20: Cryptography

-Introduces cryptographic concepts and techniques, essential for securing information and communications in cybersecurity.

These modules delve into various aspects of network security and provide a comprehensive foundation for securing today's complex IT landscapes. This well-rounded curriculum equips professionals with the knowledge and skills needed to identify, analyze, and address vulnerabilities across diverse IT environments.

Hands on Learning:

The CEH v12 program offers an immersive learning experience through over **220 hands-on labs.** These labs utilize a web-accessible cyber range equipped with real machines, vulnerable targets, and **over 3,500 industry-standard hacking tools.** This allows you to gain practical experience with the latest security vulnerabilities, common operating systems, and the most widely used security tools in cybersecurity.

What's Covered:

100% virtualization for a complete learning experience

Wide range of target platforms to hone your skills

519 attack techniques

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!

Objective-oriented flags for critical thinking and applied knowledge assessment

Cloud-based cyber range

Updated OS

Windows 11	**Windows Server 2022**
Parrot Security	**Windows Server 2019**
Android	**Ubuntu Linux**

Course Content

3000+ Student Manual Pages	**1900+** Lab Manual Pages
3500+ Hacking & Security Tools	**220** Hands-On Lab Practicals
519 Attack Techniques	**20** Refreshed Modules


C|EH®
v12
CERTIFIED ETHICAL HACKER
www.Securityorigin.com