C|EH™ v12

Certified Ethical Hacker

The Ultimate Ethical Hacking Certificate

EC-Council | ALJHOOD® مجموعة الجهود المشتركة

EC-Council Accredited Training Center

Ethical Hacking

In the dawn of international conflicts, terrorist organizations funding cybercriminals to breach security systems, either to compromise national security features or to extort huge amounts by injecting malware and denying access. Resulting in the steady rise of cybercrime. Organizations face the challenge of updating hack-preventing tactics, installing several technologies to protect the system before falling victim to the hacker.

New worms, malware, viruses, and ransomware are primary benefit are multiplying every day and is creating a need for ethical hacking services to safeguard the networks of businesses, government agencies or defense.

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization. They use this process to prevent cyberattacks and security breaches by lawfully hacking into the systems and looking for weak points. An ethical hacker follows the steps and thought process of a malicious attacker to gain authorized access and test the organization's strategies and network.

An attacker or an ethical hacker follows the same five-step hacking process to breach the network or system. The ethical hacking process begins with looking for various ways to hack into the system, exploiting vulnerabilities, maintaining steady access to the system, and lastly, clearing one's tracks.

EC-Council

The International Council of Electronic Commerce Consultants

is an American organization that offers cybersecurity certification , education, training, and services in various cybersecurity skills. EC-Council is headquartered in Albuquerque, New Mexico, and has certified over 237,000 professionals from 145 countries.

It offers professional certifications for the IT security field, such as Certified Network Defender (CND), Certified Ethical Hacker (CEH), Certified Chief Information Security Officer (CCISO), and Computer Hacking Forensics Investigator (CHFI). It also offers certifications in fields related to IT security, including disaster recovery, software security, digital forensics, and General IT security knowledge.

350
SUBJECT MATTER EXPERTS INVOLVED IN COURSE DEVELOPMENT

3,000
TOOLS & TECHNOLOGIES

220,000
CERTIFIED PROFESSIONALS

145
COUNTRIES

About C|EH

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 **12th version**, **CEH** continues to evolve with the latest operating systems, tools, tactics, exploits, and technologies.

Introducing All New C|EHv12

is a renewed program that teaches you everything you need to know about ethical hacking with training, labs, assessment, a mock engagement(practice) and even a series of global hacking competitions – all part of the C|EHV12!

C|EH v12 has designed a new learning framework that uses a -4phase methodology that includes:

Courseware | Cyber Range

Gain Skills

Cyber Range

Gain Experience

ANSI Accredited Exam

Gain Recognition

Hackerverse™

Gain Respect

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.

C|EH Skills Covered

- Network packet analysis
- Advanced log management
- Advanced hacking concepts
- Mobile and web technologies
- IDS firewalls and honeypots
- Trojans backdoors and countermeasures

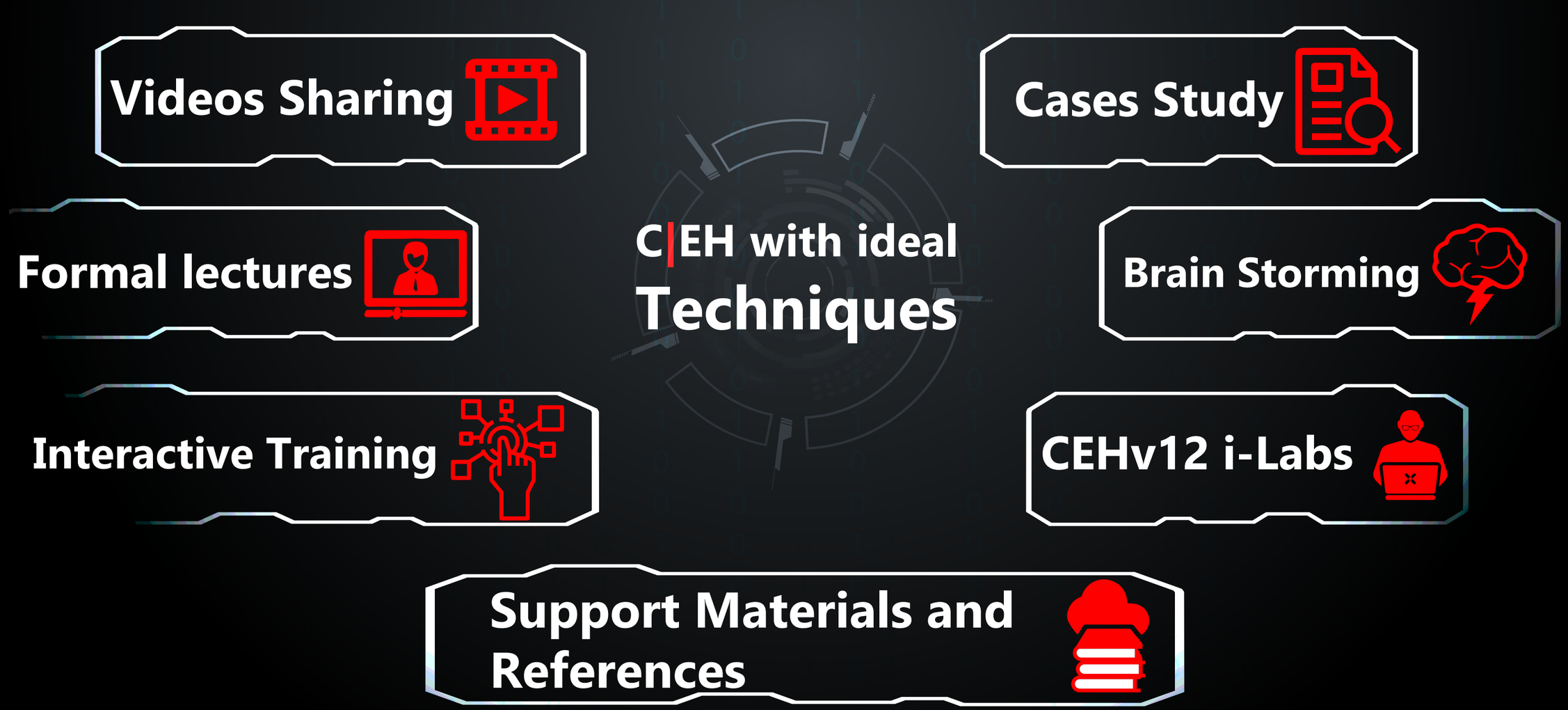
C|EH Organizational Impact

EC-Council believes in giving back to the security community as it has partaken of it. When you are a Certified Ethical Hacker, you are more than a security auditor or a vulnerability tester or a penetration tester alone. You are exposed to security checklists that will help you audit the organization's information assets, tools which will check for vulnerabilities that can be exploited and above all a methodology to assess the security posture of your organization by doing a penetration test against it. In short, the knowledge you will acquire has practical value to make your work place a more secure and efficient one.

C|EH

Demanded by Employers ... Respected by Peers

The Certified Ethical Hacker **(C|EH)** credentialing and provided by **EC-Council** is a respected and trusted ethical hacking program in the industry. Since the inception of Certified Ethical Hacker in 2003, the credential has become one of the best options for industries and companies across the world. The C|EH exam is ANSI 17024 compliant, adding value and credibility to credential members. It is also listed as a baseline certification in the US Department of Defense (DoD) Directive 8570 and is a NSCS Certified Training.



Are you Eligible for C|EH?

To be eligible , the candidate has two options:

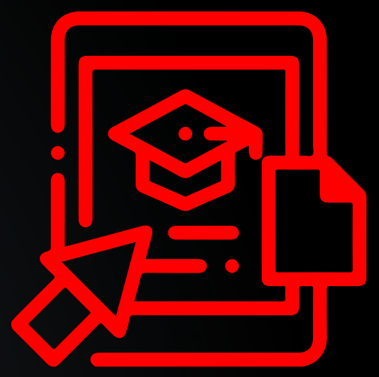
Attend Official Network Security Training by EC-Council:

If a candidate has completed an official EC-Council training either at an Accredited Training Center, via the i-Class platform, or at an approved academic institution, the candidate is eligible to challenge the relevant EC-Council exam without going through the application process.

Attempt the Exam without Official EC-Council Training:

In order to be considered for the EC-Council CEH exam without attending official network security training, the candidate must have at least 2 years of work experience in the Information Security domain. If the candidate has the required work experience, they can submit an eligibility application form along with USD 100.00, a non-refundable fee.

C|EH Exam:



Exam Language: English
Exam Duration: 4 Hours
Exam Type: Multiple Choice
Total Number of Questions: 125
Exam Prefix: 50-312 (ECC EXAM), 50-312 (VUE)

Exam Pass Score: EC-Council Exams are provided in multiple forms .
To ensure each form has equal assessment standards, cut scores are set on a “per exam form” basis. Depending on which exam form is challenged, cut scores can range from **%60** to **%85**.

System Administrators.

Information Security Analyst / Administrator.

Network Administrators and Engineers.

Information Assurance (IA) Security Officer.

C|EH

Audience ideal

Risk / Threat/ Vulnerability Analyst.

Information Security Professionals / Officers.

Information Security / IT Auditors.

Information Security Manager / Specialist.

Information Systems Security Engineer / Manager

Takeaways

Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards

Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.

Perform foot printing and reconnaissance using the latest foot printing techniques and tools as a critical pre-attack phase required in ethical hacking.

System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.

Enumeration techniques and enumeration countermeasures. Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.

Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.

Social engineering techniques and how to identify theft attacks to audit human level vulnerabilities and suggest social engineering countermeasures.

Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.

Network scanning techniques and scanning countermeasures.

Network scanning techniques and scanning countermeasures.

Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.

Session hijacking techniques to discover network-level session management,authentication/authorization, cryptographic weaknesses, and countermeasures.

DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.

Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.

Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.

Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.

SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.

Cloud computing concepts (Container technology, server-less computing), various threats/attacks, and security techniques and tools.

Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.

Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.

Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.

Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.

C|EH Training Modules

- Module "1": Introduction to Ethical Hacking
- Module "2": Foot printing and Reconnaissance
- Module "3": Scanning Networks
- Module "4": Enumeration
- Module "5": Vulnerability Analysis
- Module "6": System Hacking
- Module "7": Malware Threats
- Module "8": Sniffing
- Module "9": Social Engineering
- Module "10": Denial-of-Service
- Module "11": Session Hijacking
- Module "12": Evading IDS, Firewalls, and Honeypots
- Module "13": Hacking Web Servers
- Module "14": Hacking Web Applications
- Module "15": SQL Injection
- Module "16": Hacking Wireless Networks
- Module "17": Hacking Mobile Platforms
- Module "18": IoT Hacking
- Module "19": Cloud Computing
- Module "20": Cryptography

leading change نقود التغيير

@aljhoodgroup www.aljhood.com