EC-Council

C|EH™
Certified Ethical Hacker
v10

CERTIFIED ETHICAL HACKER v10

CERTIFIED ETHICAL HACKER (PRACTICAL)

Course Description

The Certified Ethical Hacker (C|EH v10) program is a trusted and respected ethical hacking training Program that any information security professional will need.

Since its inception in 2003, the Certified Ethical Hacker has been the absolute choice of the industry globally. It is a respected certification in the industry and is listed as a baseline certification on the United States Department of Defense Directive 8570. The C|EH exam is ANSI 17024 compliant adding credibility and value to credential members.

C|EH is used as a hiring standard and is a core sought after certification by many of the Fortune 500 organizations, governments, cybersecurity practices, and a cyber staple in education across many of the most prominent degree programs in top Universities around the globe.

Hundreds of Thousands of InfoSec Professionals as well as Career Starters have challenged the exam and for those who passed, nearly all are gainfully employed with successful careers, but the landscape is changing. Cyber Security as a profession is evolving, the barrier to entry is rising, the demand for Skilled Cyber professionals continues to grow, but it is being refined, demanding a higher level of skill and ability.

EC-Council raises the bar again for ethical hacking training and certification programs with the all new C|EH v10!

This course in its 10th iteration, is updated to provide you with the tools and techniques used by hackers and information security professionals alike to break into any computer system. This course will immerse you into a “Hacker Mindset” in order to teach you how to think like a hacker and better defend against future attacks. It puts you in the driver’s seat with a hands-on training environment employing a systematic ethical hacking process.

You are constantly exposed to creative techniques of achieving optimal information security posture in the target organization; by hacking it! You will learn how to scan, test, hack and secure target systems. The course covers the Five Phases of Ethical Hacking, diving into Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

The tools and techniques in each of these five phases are provided in detail in an encyclopedic approach and absolutely no other program offers you the breadth of learning resources, labs, tools and techniques than the C|EH v10 program.

> *EC-Council has further improved my technical skill. As a result, it has enabled me to provide more details / in-depth analysis to identify any security gaps in the IT infrastructure.*
>
> ***Chin Wen-Sing,***
> *Shell IT International*

C|EH™
Certified Ethical Hacker

Target Audience

Ethical hackers, System Administrators, Network Administrators and Engineers, Webmanagers, Auditors, Security Professionals in general.

Suggested Duration

5 days (9am – 5pm)
Minimum 40 hours

Certification

The C|EH exam can be challenged post the completion of attending the complete official C|EH course. Candidates that successfully passes the exam will receive their C|EH certificate and membership privileges. Members are expected to adhere to recertification requirements through EC-Council's Continuing Education Requirements.

As a powerful addition to the C|EH exam, the new C|EH (Practical) exam is now available adding even more value to the C|EH certification through practical validation of skills and abilities.

Attaining Industry Trusted and Preferred Credentials C|EH and C|EH (Practical)

The C|EH exam is ANSI compliant, earning with that the respect and trust of employers globally. Today, you can find C|EH credential professionals in over 145 countries working with some of the biggest and finest corporations across industries including government, military, financial, healthcare, energy, transport and many more.

C|EH (ANSI)

- **Exam Title:** Certified Ethical Hacker (ANSI)
- **Exam Code:** 312-50 (ECC EXAM), 312-50 (VUE)
- **Number of Questions:** 125
- **Duration:** 4 hours
- **Availability:** ECCEXAM / VUE
- **Test Format:** Multiple Choice
- **Passing Score:** Please refer to https://cert.eccouncil.org/faq.html

C|EH (PRACTICAL)

- **Exam Title:** Certified Ethical Hacker (Practical)
- **Number of Practical Challenges:** 20
- **Duration:** 6 hours
- **Availability:** Aspen- iLabs
- **Test Format:** iLabs cyber range
- **Passing Score:** 70%

The C|EH (Practical) is a 6 hours practical exam built to exacting specifications by subject matter experts in the EH field. Professionals that possess the C|EH credential will be able to sit for exam that will test their limits in unearthing vulnerabilities across major operating systems, databases, and networks. To those who meet and exceed the skills level set, they will earn the new industry required certification – the C|EH (Practical) certification.

C|EH (Practical) is available fully proctored, online, with remote facilities globally.

The combined benefit of a practical exam that is fully proctored anywhere in the world will provide organizations with a skills-validated and trusted credential when employing cybersecurity professionals. With its global availability, organizations can now quickly train, test and deploy a cyber-ready workforce effectively.

Eligibility Criteria

- Be a CEH member in good standing (Your USD 100 application fee will be waived);
- or Have a minimum of 3 years working experience in InfoSec domain (You will need to pay USD 100 as a non-refundable application fee);
- or Have any other industry equivalent certifications such as OSCP or GPEN cert (You will need to pay USD 100 as a non-refundable application fee).

C|EH v10 Recognition / Endorsement / Mapping

The National Initiative for Cybersecurity Education (NICE)

American National Standards Institute (ANSI)

Committee on National Security Systems (CNSS)

United States Department of Defense (DoD)

National Infocomm Competency Framework (NICF)

Department of Veterans Aairs

KOMLEK

MSC

After attending the C|EH course, my company has had more confidence to assign me penetration testing tasks regularly. .....and the penetration testing conducted by third party uses my direction and our security policies.

Arif Jatmoko,
Coca-Cola

Top 10 Critical Components of C|EH v10

1. 100% Compliance to NICE 2.0 Framework

C|EH v10 maps 100 percent to NICE framework's Protect and Defend specialty area

2. Inclusion of New Module

Vulnerability Analysis

Learn how to perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems. This module covers the vulnerability management life cycle, and various approaches and tools used to perform the vulnerability assessment.

IoT Hacking

Understand the potential threats to IoT platforms and learn how to defend IoT devices securely.

3. Focus on Emerging Attack Vectors (e.g., Cloud, AI, ML, etc.)

C|EH provides an insight into cloud computing threats and cloud computing attacks. It discusses cloud computing security and the necessary tools. It provides an overview of pen-testing steps which an ethical hacker should follow to perform a security assessment of the cloud environment.

Artificial Intelligence (AI) is an emerging solution used in defending networks against various attacks that an antivirus scan cannot detect. Learn how this can be deployed through the C|EH course.

4. Hacking Challenges at the End of Each Module

Challenges at the end of each modules ensures you can practice what you have learnt. They help student understand how knowledge can be transformed as skills and can be used to solve real-life issues.

5. Coverage of latest Malware

The course is updated to include the latest ransomware, banking and financial malware, IoT botnets, Android malwares and more!

6. Inclusion of complete Malware Analysis Process

Discover and learn how to reverse engineer malware in order to determine the origin, functionality, and potential impact of a malware. By performing malware analysis, the detailed information regarding the malware can be extracted, analysed and this is a crucial skill of an ethical hacker.

7. Hands-on Program

More than 40 percent of class time is dedicated to the learning of practical skills and this is achieved through EC-Council labs. Theory to practice ratio for C|EH program is 60:40 providing students with a hands-on experience of the latest hacking techniques, methodologies, tools, tricks, etc.

C|EH comes integrated with labs to emphasize the learning objectives. It also provides additional labs that students can practice post training on their own time, through EC-Council's iLabs platform which students can purchase separately.

8. Lab environment simulates a real-time environment

C|EH v10 lab environment consists of latest operating systems including Windows Server 2016 and Windows 10 configured with Domain Controller, firewalls, and vulnerable web applications for honing the skills of hacking.

9. Covers latest hacking tools (Based on Windows, MAC, Linux, and Mobile)

The C|EH v10 course includes a library of tools that is required by security practitioners and pentesters to find uncover vulnerabilities across different operation platforms. This provides a wider option to students than any other programs in the market.

10. ANSI Accreditation

ANSI accreditation signifies that the certification holder has completed a prescribed course of study designed specifically to meet predefined industry requirements

> *Thank you for your holistic approach in security which gives much in sight about various security tools. A must for security evangilist to defence their information golden eggs.*
>
> ***Gatta Sambasiva Rao,***
> *Tata Consultancy Services*

We are involved in a project that uses the techniques for performing Vulnerability assessment .The Certified Ethical hacker certification has immensely contributed to enhance my skills.

Manoj Kumar K,
IBM Global Services

Course Outline

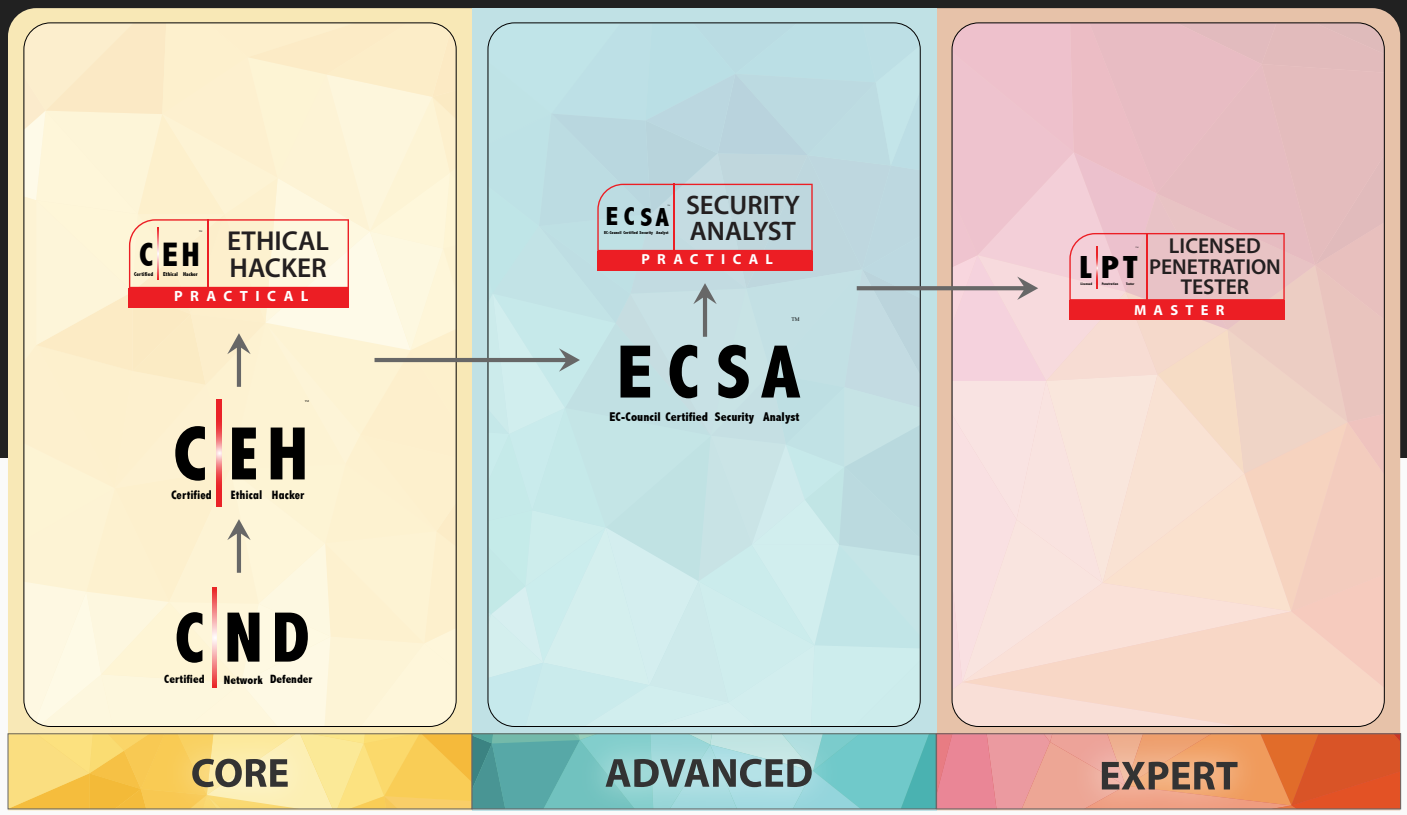
- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

What will you learn?

1. Key issues plaguing the information security world, incident management process, and penetration testing.
2. Various types of footprinting, footprinting tools, and countermeasures.
3. Network scanning techniques and scanning countermeasures.
4. Enumeration techniques and enumeration countermeasures.
5. System hacking methodology, steganography, steganalysis attacks, and covering tracks.
6. Different types of Trojans, Trojan analysis, and Trojan countermeasures.
7. Working of viruses, virus analysis, computer worms, malware analysis procedure, and countermeasures.
8. Packet sniffing techniques and how to defend against sniffing.
9. Social Engineering techniques, identify theft, and social engineering countermeasures.
10. DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures.
11. Session hijacking techniques and countermeasures.
12. Different types of webserver attacks, attack methodology, and countermeasures.
13. Different types of web application attacks, web application hacking methodology, and countermeasures.
14. SQL injection attacks and injection detection tools.
15. Wireless Encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
16. Mobile platform attack vector, android vulnerabilities, mobile security guidelines, and tools.
17. Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures.
18. Various cloud computing concepts, threats, attacks, and security techniques and tools.
19. Different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.
20. Various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
21. Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
22. Different threats to IoT platforms and learn how to defend IoT devices securely.

EC-Council VAPT Learning Track

EC-Council's cybersecurity programs and credentials are organized into tracks to allow professionals to specialize in a particular domain or gain advancements with added recognition and skills, one after the other.



CND is the world's most advanced network defense course that covers 14 of the most current network security domains any individuals will ever want to know when they are planning to protect, detect, and respond to the network attacks. The course contains hands-on labs, based on major network security tools and to provide network administrators real world expertise on current network security technologies and operations.

C|EH is the world's most advanced ethical hacking course covering 20 of the most important security domains any individual will need when they are planning to beef-up the information security posture of their organization. The course provides hacking techniques and tools used by hackers and information security professionals.

To provide employers with the confidence that you not only know your stuff, but can do the job, challenge the C|EH (Practical) exam to proof your skills.

C|EH Certified Ethical Hacker ..... CERTIFIED ETHICAL HACKER

ECSA is a globally respected penetration testing program that covers the testing of modern infrastructures, operating systems, and application environments while teaching the students how to document and prepare professional penetration testing report. This program takes the tools and techniques covered in C|EH to next level by utilizing EC-Council's published penetration testing methodology.

Employers can today trust not only know your knowledge in pentesting, but your skills when you produce your ECSA (Practical) credential to proof your skills.

The Advanced Penetration Testing program is the capstone to EC-Council's entire information security track, right from the C|EH to the ECSA Program. The course brings advanced pentesting skills not covered in the ECSA course offering students even more advanced techniques employed by experienced pentesters.

The LPT (Master) exam covers the entire Penetration Testing process and lifecycle with keen focus on report writing, required to be a true professional Penetration Tester.

Each program offers domain specific knowledge, training and ability to prepare a professionals through their job requirements bringing career advancement and opportunities.

Click on this link to find out more details about each certification and complete the VAPT track to attain industrys' most sought after credentials.

> *"Truly an excellent course full of in depth knowledge and powerful suite of tools that a hacker may use and how a hacker's mindset works. This course reveals how easy it is for a hacker to compromise applications, networks, servers without leaving a trace. This course helped me take preemptive measures against hackers simply by 'thinking like a hacker' and ensuring in my day to day activities that no matter what I am doing always be aware of a security. Having the C|EH certification has giving me and my customers the confidence that security is of my highest priorities when it comes to developing solutions. This course has giving me extremely valuable knowledge that will stick with me for a long time to come. I highly recommend this course to any I.T. professionals who take their security serious both as an individual and for their organization they work for."*
>
> ***Jason O'Keefe,***
> *Hewlett-Packard Company, Ireland*

EC-Council

www.eccouncil.org