
e.KRAAL
INNOVATION HUB
C.E.H
CERTIFIED
ETHICAL
HACKER
The Gold Standard in Ethical Hacking Credentials

## Certified Ethical Hacker v10: Course Description

The Certified Ethical Hacker 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. In fact, 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 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.

This course 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 trained on creative hacking techniques to achieve optimal information security posture in any target organization! 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 encyclopaedic approach and absolutely no other program offers you the breadth of learning resources, labs, tools and techniques than the C|EH program.

## Certified Ethical Hacker (Practical)

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

C|EH (Practical) is available only as an online and fully proctored exam because we insist that that is the only way quality can be assured. EC-Council is the first in the world to offer a fully online, remote proctored practical exam.

The overall benefit of a practical exam that it is fully proctored anywhere in the world and 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.

## C|EH (Master)

To be placed at the tip of your organization's cyber spear, you must be confident, proficient in your job, and be at the top of your game. You must be able to think on your feet, act quickly, appropriately, and proportionally. Make a mistake and bad things can happen.

C|EH Master gives you the opportunity to prove your capabilities and skills to the industry at large, your employer, and your peers that you can in fact take on and overcome challenges as an Ethical Hacker.

To prove that you are skills-proficient in Ethical Hacking, we don't give you exam simulations. Many other certification providers talk about Performance Based Assessments, but the reality is far from them testing your skills on a real-life environment. Most of these 'performance based tests' are limited to simulations or interactive ways of theoretically testing your knowledge.

We test your abilities with real-world challenges in a real-world environment, using labs and tools requiring you to complete specific ethical hacking challenges within a time limit, just as you would face in the real world! In the EC-Council C|EH (Practical) exam, a complex network of a large organisation, consisting of various network systems (including DMZ, Firewalls etc.) is replicated, where you as an ethical hacker, have to discover and exploit real time vulnerabilities while also auditing the systems. This is a rare offering, since very few certifications create such environments, while others (including respected brands) only claim to provide hands-on learning and can't provide experiential learning that's akin to actually performing the ethical hacking techniques learnt, while working in real life.

*It is one thing to read about how the different hacking techniques work, but it is good to see a professional use them in the lab situation.*

***- David Kane,***
*Officer at the US Army*


## Who is it for?

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

## Suggested Course Duration

5 Days (9AM to 5 PM)
Minimum 40 hours

## C|EH Certification

C|EH exam validates the certification holder's knowledge in ethical hacking principles and countermeasure techniques.

## C|EH (Practical) Certification

The C|EH (Practical) exam tests the skills of a candidate in a 6-hour, rigorous scenario-based exam that challenges the ethical hacker with real life hacking situations. This creates an ideal environment to gain useful, real-world skills.

## C|EH Master

C|EH Master, is the next evolution for the world-renowned Certified Ethical Hacker credential, and a logical 'next step' for those holding the prestigious certification. Earning the C|EH Master designation is your way of saying, "***I learned it, I understood it, and I proved it.***"

## How to attain the C|EH (Master) Credential

To earn the C|EH Master credential, you must successfully demonstrate your knowledge of and skill in Ethical Hacking through two challenging rounds of exams.

### C|EH

- **Exam Title:** Certified Ethical Hacker
- **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.htm

### 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%

Clause: Age Requirements and Policies Concerning Minors

**The age requirement for attending the training or attempting the exam is restricted to any candidate that is at least 18 years old.**

First, you must pass the Accredited Certified Ethical Hacker (C|EH) knowledge-based exam. The C|EH exam is compliant, earning the respect and trust of employers globally.
Once you complete this first step, you can move on to earning the C|EH (Master) designation via the C|EH (Practical) Exam. The C|EH (Practical) Exam was developed to give Ethical Hackers the chance to prove their skills and abilities using a cyber range containing real world challenges.
Today, you can find C|EH credentialed 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.

### Eligibility Criteria for C|EH (Practical) exam

There is no predefined eligibility criteria for those interested in attempting the C|EH (Practical) exam besides being at least 18 years old. You can purchase the exam dashboard code here.

The age requirement for attending the training or attempting the exam is restricted to any candidate that is at least 18 years old.

**Note:** The exam dashboard code is valid for 3 months from date of receipt.

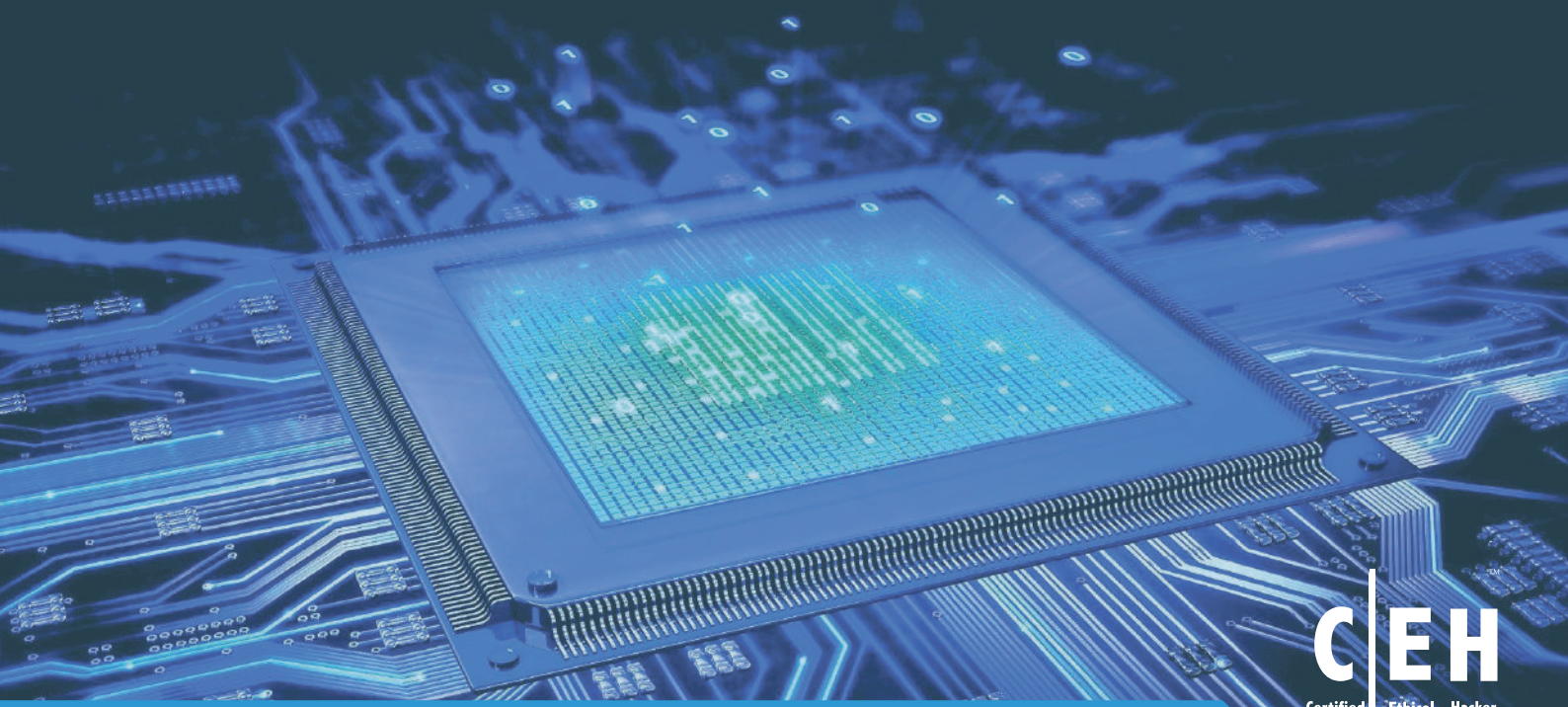
### Application Process

In order to proceed with the exam the steps below will need to be completed:

- The exam dashboard code can be purchased here

- Upon successful purchase, the candidate will be sent the exam dashboard code with instructions to schedule the exam.

Should you require the exam dashboard code validity to be extended, contact practicals@eccouncil.org before the expiry date. Only valid and active codes can be extended..



C|EH Certified Ethical Hacker MASTER

## Your Road Map to C|EH (Master)

C|EH Master, is the next evolution for the world-renowned Certified Ethical Hacker credential, and a logical 'next step' for those holding the prestigious certification. Earning the C|EH Master designation is your way of saying, "I learned it, ***I understood it, and I proved it."***

## 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 Affairs


KOMLEK


MSC


GCHQ

*I find that the C|EH credential carries a lot of weight in the professional environment and is proof of your practical knowledge.*

***- Shane Mitchell,***
*Senior Network Analyst at*
*Ontario Ministry of Government and Consumer Services*

# 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 modules

### 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

## 3 Focus on emerging attack vectors (e.g., Cloud, AI, ML, etc.)

This section provides insight into cloud computing threats and cloud computing attack-sIt discusses cloud computing security and the necessary tools. It also 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 module, ensure you can practice what you have learned. They help students understand how to apply knowledge and skills 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 malware and more!

## 6 Inclusion of complete malware analysis process

Learn how to reverse engineer malware in order to determine the origin, functionality, and potential impact. Extracting and analyzing malware data and this is a crucial skill for 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. The theory to practice ratio for C|EH program is 60:40, providing students with a hands-on experience of the latest hacking techniques, methodologies and tools. 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

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

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

The C|EH v10 course includes a library of tools used by security practitioners and pentesters to find uncover vulnerabilities across different operation platforms, providing candidates with more tools than any other programs in the market.

## 10 Accreditation

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

## CourseOutline

- 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

*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.*

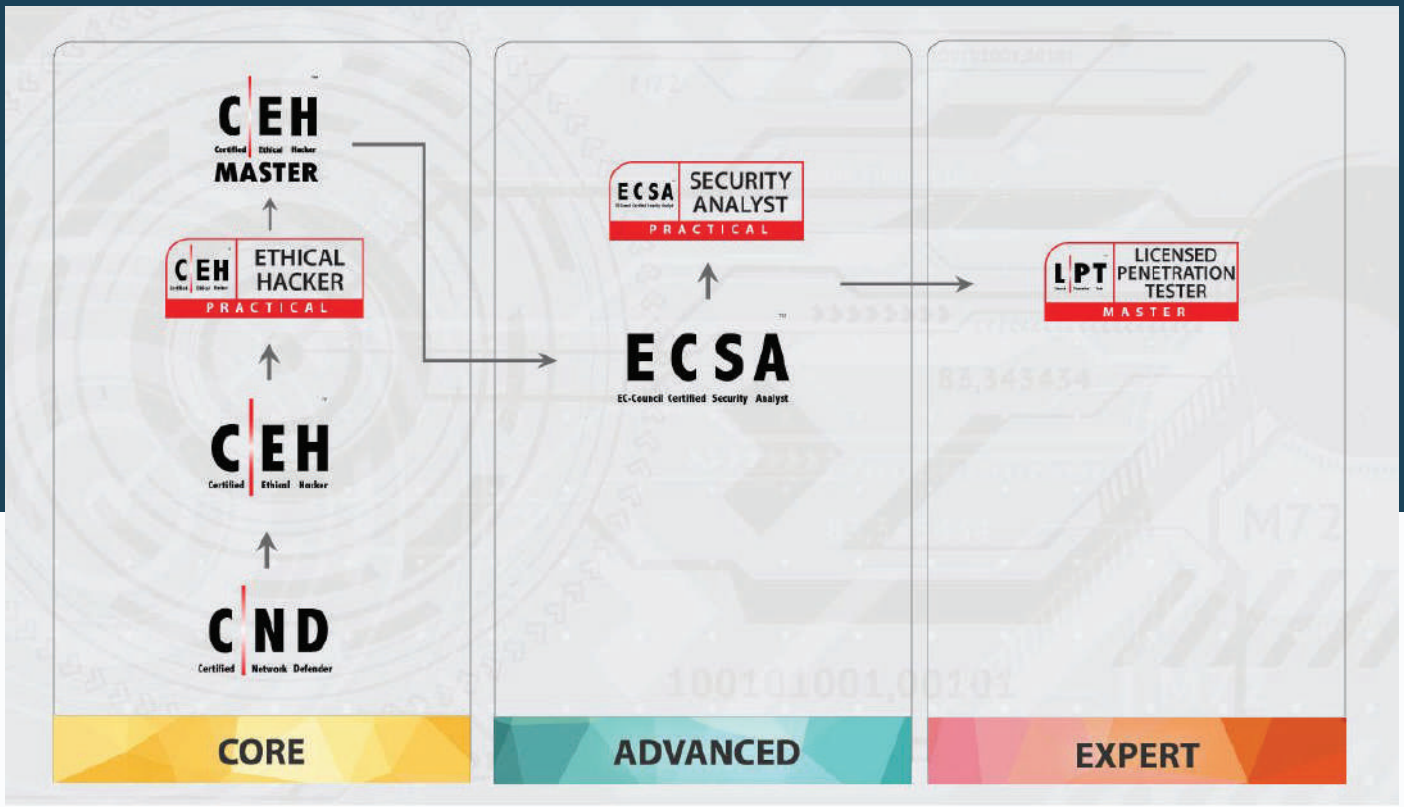
***Manoj Kumar K,***
*IBM Global Services*

## What will you learn?

1. Key issues plaguing the information security world, incident management processes, and penetration testing
2. 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 the processes involved in covering tracks
6. 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. Webserver attacks, attack methodology, and countermeasures
13. 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 vectors, android vulnerabilities, mobile security guidelines, and tools
17. Firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures
18. Cloud computing concepts, threats, attacks, and security techniques and tools
19. Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools
20. Penetration testing, security audit, vulnerability assessment, and the penetration testing roadmap
21. Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems
22. Threats to IoT platforms and how to defend IoT devices

## 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. It covers 14 of the most current network security domains you need to know to protect, detect, and respond to network attacks. It contains hands-on labs based on major network security tools to provide network administrators real world expertise on current network security technologies and operations is the world's most advanced network defense course. 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 improve the information security posture of their organization. The course provides hacking techniques and tools used by criminals as well as 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 prove your skills.

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

---

The Advanced Penetration Testing program is the capstone to EC-Council's entire information security track, which starts with the C|EH and ends with the ECSA Program. The LPT 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 and training to prepare a professionals for the job requirements that can bring career advancement and opportunities.

Click on this link to find out more 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*

e.KRAAL

INNOVATION HUB