Module Title : Certified Ethical Hacker v12 Master
Duration : 5 days

Overview

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.

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: 1. Learn 2. Certify 3. Engage 4. Compete.

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.

The C|EH® v12 is a specialized and one-of-a-kind training program to teach you everything you need to know about ethical hacking with hands-on training, labs, assessment, a mock engagement (practice), and global hacking competition. Stay on top of the game with the most in-demand skills required to succeed in the field of cybersecurity.

1. LEARN

- 5 days of training
- 20 modules
- 3000+ pages of student manual
- 1900+ pages of lab manual
- Over 200 hands-on labs with competition flags
- Over 3,500 hacking tools - Learn how to hack multiple operating 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

2. CERTIFY

C|EH® ANSI

- 125 Multiple-Choice Questions
- 4 hours

C|EH® Practical

- 6-hour Practical Exam
- 20 Scenario-Based Questions

3. ENGAGE

- Conduct a real-world ethical hacking assignment
- Apply the 5 phases
  - Reconnaissance
  - Scanning
  - Gaining Access
  - Maintaining Access
  - Covering Your Tracks

4. COMPETE

- New challenges every month
- 4-hour competition
- Compete with your peers all over the world
- Hack your way to the top of the leaderboard
- Gain recognition
- Challenges include:
  - OWASP Top 10 Web Application Threat Vectors
  - Ransomware/ Malware Analysis
  - Outdated/Unpatched Software
  - System Hacking and Privilege Escalation

  - Web Application Hacking and Pen Testing
  - Cloud Attack/Hacking
  - and many more...

What You Will Learn

C|EH is divided into 20 modules and delivered through a carefully curated training plan that typically spans across 5 days. As you progress through your training, each module offers extensive hands-on lab components that allow you to practice the techniques and procedures taught in the program in real-time on live machines.

Ethical Hacking Labs

With over 220 hands-on labs, conducted in our cyber range environment, you will have the opportunity to practice every learning objective in the course on live machines and vulnerable targets. Pre-loaded with over 3,500 hacking tools and a variety of operating systems, you will gain unprecedented exposure to and hands-on experience with the most common security tools, latest vulnerabilities, and widely used operating systems on the market. Our range is web accessible, allowing you to study and practice from anywhere with a connection.

Prerequisites

There are no specific prerequisites for the C|EH program, however we strongly recommend candidates possess a minimum of 2 years' experience in IT security before joining a C|EH training program. C|EH training is about testing systems and using them for purposes not originally intended, candidates should understand the basic functions of those IT systems before attempting to hack them. (Example: C|EH will teach the process of host evaluation leading to enumeration, in this process trainees will scan downrange targets using common scanning techniques such as Nmap which will respond with a list of ports, enumerating those ports and the services running on them can be used to expose common vulnerabilities and weaknesses in systems. The C|EH program will not teach you what a port is, that is essential knowledge you must have to be successful in the class.) If you do not possess the foundational skills in IT and Networking, we recommend starting with our free cybersecurity Essentials Series found here: https://www.eccouncil.org/academia/essentials

Target Audience

- 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

Course Agenda

Time	Day 1	Day 2	Day 3	Day 4	Day 5
9:00am - 10:30am	Module 1	Module 5	Module 9	Module 13	Module 17
10:30am - 10:45am	Morning Break	Morning Break	Morning Break	Morning Break	Morning Break
10:45am - 12:30pm	Module 2	Module 6	Module 10	Module 14	Module 18
12:30pm - 1:30pm	Lunch Break	Lunch Break	Lunch Break	Lunch Break	Lunch Break
1:30pm - 3:30pm	Module 3	Module 7	Module 11	Module 15	Module 19
3:30pm - 3:45pm	Afternoon Break	Afternoon Break	Afternoon Break	Afternoon Break	Afternoon Break
3:45pm - 5:00pm	Module 4	Module 8	Module 12	Module 16	Module 20

Course Outline

Module 01: Introduction to Ethical Hacking

Module 02: Foot Printing and Reconnaissance

Module 03: Scanning Networks

Module 04: Enumeration

Module 05: Vulnerability Analysis

Module 06: System Hacking

Module 07: Malware Threats

Module 08: Sniffing
Module 09: 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 and OT Hacking
Module 19: Cloud Computing
Module 20: Cryptography

Content Included

- eCourseware
- Exam Voucher*
- Next version of eCourseware
- 6 months of official labs
- C|EH Engage
- Global C|EH Challenges
- Exam Preparation
- C|EH Practical Exam
- 10 Ethical Hacking Video Library
- 4 Exam Retakes**

**Exam retakes are included with every courseware package. Candidates may activate this benefit through the EC-Council student portal (ASPEN)*

*** Proctor administration fees will be applicable for each attempt of the retake examination*