

CEH: Certified Ethical Hacker v13

Overview

The Certified Ethical Hacker (CEH) provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. CEH v13 powered with AI capabilities will teach you how hackers think and act so you will be better positioned to set up your security infrastructure and defend against attacks. By providing an understanding of system weaknesses and vulnerabilities, the CEH course helps students learn to protect their organizations and strengthen their security controls in order to minimize the risk of a malicious attack.

CEH v13 powered with AI capabilities was built to incorporate a hands-on environment and systematic process across each ethical hacking domain and methodology, giving you the opportunity to work toward proving the required knowledge and skills needed to achieve the CEH credential and perform the job of an ethical hacker.

Course Objectives

CEH 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.

Duration

5 Days

CEH: Certified Ethical Hacker v13

Who Should Attend

- 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

Prerequisites

There are no specific prerequisites for the CEH program, however we strongly recommend candidates possess a minimum of 2 years' experience in IT security before joining a CEH training program. CEH 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: CEH 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 CEH 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>

CEH: Certified Ethical Hacker v13

Course Topics

Module 1	Introduction to Ethical Hacking Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.
Module 2	Foot Printing and Reconnaissance Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking
Module 3	Scanning Networks Learn different network scanning techniques and countermeasures.
Module 4	Enumeration Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures.
Module 5	Vulnerability Analysis Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools are also included.
Module 6	System Hacking Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks.
Module 7	Malware Threats Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.
Module 8	Sniffing Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.

CEH: Certified Ethical Hacker v13

Module 9	Social Engineering Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.
Module 10	Denial-of-Service Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.
Module 11	Session Hijacking Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.
Module 12	Evading IDS, Firewalls and Honeypots Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.
Module 13	Hacking Web Servers Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.
Module 14	Hacking Web Applications Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures.
Module 15	SQL Injection Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.
Module 16	Hacking Wireless Networks Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.

CEH: Certified Ethical Hacker v13

Module 17	Hacking Mobile Platforms Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.
Module 18	IoT and OT Hacking Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.
Module 19	Cloud Computing Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools.
Module 20	Cryptography Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

CEH: Certified Ethical Hacker v13

Time	Day 1
9:00am - 10:30am	Module 1: Introduction to Ethical Hacking
10:30am - 10:45am	Morning Break
10:45am - 12:30pm	Module 2: Foot Printing and Reconnaissance
12:30pm - 1:30pm	Lunch Break
1:30pm - 3:30pm	Module 3: Scanning Networks
3:30pm - 3:45pm	Afternoon Break
3:45pm - 5:00pm	Module 4: Enumeration

Time	Day 2
9:00am - 10:30am	Module 5: Vulnerability Analysis
10:30am - 10:45am	Morning Break
10:45am - 12:30pm	Module 6: System Hacking
12:30pm - 1:30pm	Lunch Break
1:30pm - 3:30pm	Module 7: Malware Threats
3:30pm - 3:45pm	Afternoon Break
3:45pm - 5:00pm	Module 8: Sniffing

Time	Day 3
9:00am - 10:30am	Module 9: Social Engineering
10:30am - 10:45am	Morning Break
10:45am - 12:30pm	Module 10: Denial-of-Service
12:30pm - 1:30pm	Lunch Break
1:30pm - 3:30pm	Module 11: Session Hijacking
3:30pm - 3:45pm	Afternoon Break
3:45pm - 5:00pm	Module 12: Evading IDS, Firewalls and Honeypots Q&A and Wrap-Up

CEH: Certified Ethical Hacker v13

Time	Day 4
9:00am - 10:30am	Module 13: Hacking Web Servers
10:30am - 10:45am	Morning Break
10:45am - 12:30pm	Module 14: Hacking Web Applications
12:30pm - 1:30pm	Lunch Break
1:30pm - 3:30pm	Module 15: SQL Injection
3:30pm - 3:45pm	Afternoon Break
3:45pm - 5:00pm	Module 16: Hacking Wireless Networks

Time	Day 5
9:00am - 10:30am	Module 17: Hacking Mobile Platforms
10:30am - 10:45am	Morning Break
10:45am - 12:30pm	Module 18: IoT and OT Hacking
12:30pm - 1:30pm	Lunch Break
1:30pm - 3:30pm	Module 19: Cloud Computing
3:30pm - 3:45pm	Afternoon Break
3:45pm - 5:00pm	Module 20: Cryptography