Zuoix

The All-New

C|EH®
Certified Ethical Hacker

1 LEARN

2 CERTIFY

3 ENGAGE

4 COMPETE

Attain the World's No.1 Credential in Ethical Hacking

Build your career with the most in-demand cybersecurity certification in the world:

THE CERTIFIED ETHICAL HACKER

The World's No. 1 Ethical Hacking Certification for 20 Years

- **Ranked #1 In Ethical Hacking Certifications by ZDNet**
- **Ranked as a Top 10 Cybersecurity Certification**
- **C|EH Ranks 4th Among Top 50 Leading Cybersecurity Certifications**

Who is a Certified Ethical Hacker?

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 CEHacker 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.

What is Certified Ethical Hacking?

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 this 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.

This course 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.

What's New in this course version?

LEARN | CERTIFY | ENGAGE | COMPETE

This course 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.

Master ethical hacking skills that go beyond the certification.

Gain Skills

Gain Recognition

Gain Experience

Gain Respect

The new learning framework covers not only a comprehensive training program to prepare you for the certification exam but also the industry's most robust, in-depth, hands-on lab and practice range experience.

Enter the Hackerverse With CEH
Enhance Your Ethical Hacking Career

1 LEARN

- 8 weeks of enhanced, hands on training
- 20 modules
- 300+ pages of student manual
- 190+ pages of lab manual
- Over 20 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

CEH ANSI

- 125 Multiple-Choice Questions
- 4 hours

CEH 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...

1 LEARN

This CEH training program includes 20 modules covering various technologies, tactics, and procedures, providing prospective ethical hackers with the core knowledge needed to thrive in cybersecurity. Delivered through a carefully curated training plan that typically spans 8 days, The course has been designed to continue to evolve to keep up with the latest OS, exploits, tools, and techniques. The concepts covered in the training program are split 50/50 between knowledge-based training and hands-on application through our cyber range. Every tactic discussed in training is backed by step-by-step labs conducted in a virtualized environment with live targets, live tools, and vulnerable systems. Through our lab technology, every participant will have comprehensive hands-on practice to learn and apply their knowledge."

20 REFRESHED MODULES

300+ PAGES OF STUDENT MANUAL

Course Outline

20 Modules That Help You Master the Foundations of Ethical Hacking and Prepare to Take the CEH Certification Exam

Module 01

Introduction to Ethical Hacking

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Module 02

Foot Printing and Reconnaissance

Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.

Module 03

Scanning Networks

Learn different network scanning techniques and countermeasures.

Module 04

Enumeration

Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, and associated countermeasures.

Module 05

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.

Module 06

System Hacking

Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

Module 07

Malware Threats

Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures.

Module 08

Sniffing

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Module 09

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, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Module 11

Session Hijacking

Understand 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

Get introduced to firewall, intrusion detection system (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.

LEARN

Module 14

Hacking Web Applications

Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

Module 15

SQL Injection

Learn about SQL injection attacks, evasion techniques, and SQL injection countermeasures.

Module 16

Hacking Wireless Networks

Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi sedcurity tools, and countermeasures.

Module 17

Hacking Mobile Platforms

Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

Module 18

IoT and sOT Hacking

Learn different types of IoT and sOT attacks, hacking methodology, hacking tools, and countermeasures.

Module 19

Cloud Computing

Learn different cloud computing concepts, such as container technologies and server less computing, various cloud computing threats, attacks, hacking methodology, 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.

HANDS-ON LEARNING LABS

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

What's Covered:

100% virtualization for a complete learning experience

After registering, you will have full access to pre-configured targets, networks, and the attack tools necessary to exploit them:

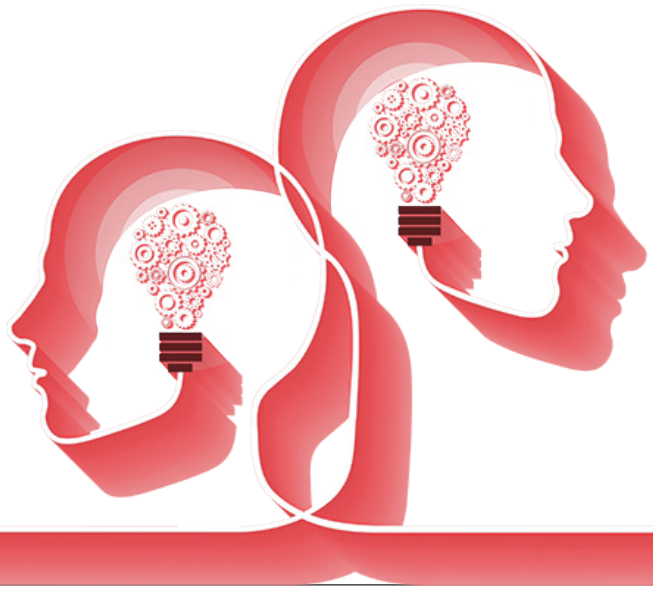
- Pre-configured vulnerable websites
- Vulnerable, unpatched operating systems
- Fully networked environments
- 3,500+ hacking tools
- And much more!

Wide range of target platforms to hone your skills

519 attack techniques

Objective-oriented flags for critical thinking and applied knowledge assessment

Cloud-based cyber range



Prove Your Skills and Abilities With Online, Practical Examinations

The Certified Ethical Hacker credential is trusted globally as the industry standard for evaluating one's understanding of ethical hacking and security testing. As an ANSI 17024 accredited examination, the 150-question, 4-hour proctored exam is recognized across the globe as the original and most trusted tactical cyber security certification for ethical hackers. Certification domains are carefully vetted through industry practitioners, ensuring the certification maps to current industry requirements; this exam undergoes regular psychometric evaluation and tuning to ensure a fair and accurate measure of the candidate's knowledge in the ethical hacking domain.

Certified Ethical Hacker (CEH) Certification

The CEH exam is a 4-hour exam with 125 multiple-choice questions. This knowledge-based exam will test your skills in information security threats and attack vectors, attack detection, attack prevention, procedures, methodologies, and more!

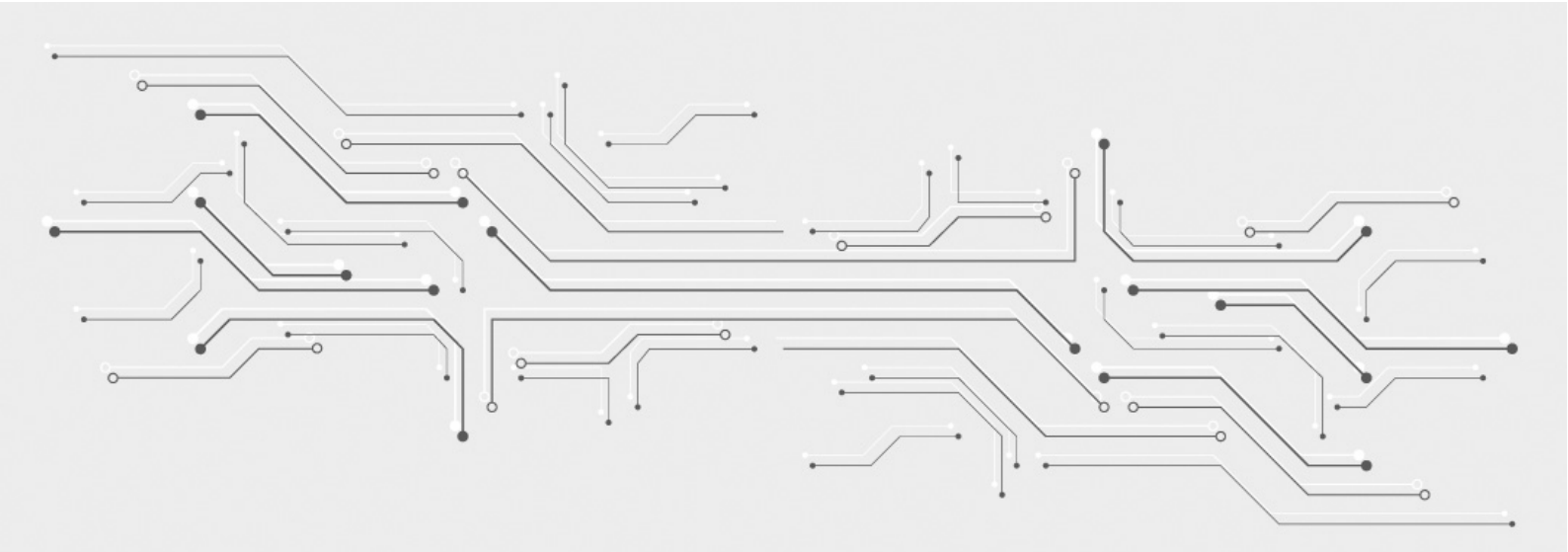
PRACTICALS

CEH Practical Certification

The CEH Practical is a 6-hour, 100% hands-on exam delivered in our Cyber Range that requires you to demonstrate skills and abilities of ethical hacking techniques such as:

- Port scanning tools (e.g., Nmap, Hping)
- Vulnerability detection
- Attacks on a system (e.g., DoS, DDoS, session hijacking, web server and web application attacks, SQL injection, wireless threats)
- SQL injection methodology and evasion techniques
- Web application security tools (e.g., Acunetix WVS)
- SQL injection detection tools (e.g., IBM Security AppScan)
- Communication protocols

This is the next step to becoming a CEH Master after you have achieved your CEH certification. Within the CEH Practical, you have limited time to complete 20 challenges to test your skills and proficiency in a performance-based cyber range. This exam is NOT a simulation and incorporates a live corporate network of VMs and applications with solutions to uncover vulnerabilities.



Zuoix

WE DON'T JUST TEACH

ETHICAL HACKING

WE BUILD CYBER CAREERS

Attain the World's No.1 Credential in Ethical Hacking