THE LEARNING CENTER
A TECHNICAL TRAINING INSTITUTION

C|EH™
CERTIFIED ETHICAL HACKER

A Certified Ethical Hacker is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s).

Skills Measured

- Establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures.
- Inform the public that credentialed individuals meet or exceed the minimum standards.
- Learn the latest hacking tools and techniques used by hackers and IS professionals

EC-Council's Certified Ethical Hacker is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

Our unique model follows a streamlined approach to workforce development and skills attainment

Assess: Assess each student to determine existing skill sets

Educate: Deliver goal-specific training utilizing all delivery modalities

Mentor: Expose students to instructors and mentors with front-line IT and cybersecurity experience

Certify: Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate: Validate student abilities through performance analytics and real-world exercises hosted on a cyber range

Exam Objectives: 312-50 CEHv11

Information Security and Ethical Hacking Overview	6%
Reconnaissance Techniques	21%
System Hacking Phases and Attack Techniques	17%
Network and Perimeter Hacking	14%
Web Application Hacking	16%
Wireless Network Hacking	6%
Mobile Platform, IoT, and OT Hacking	8%
Cloud Computing	6%
Cryptography	6%

Course Outline:

Chapter 1: Introduction to Ethical Hacking
Chapter 2: Footprinting and Reconnaissance
Chapter 3: Scanning Networks
Chapter 4: Enumeration
Chapter 5: Vulnerability Analysis
Chapter 6: System Hacking
Chapter 7: Malware Threats
Chapter 8: Sniffing
Chapter 9: Social Engineering
Chapter 10: Denial of Service
Chapter 11: Session Hijacking
Chapter 12: Evading IDS, Firewalls, and Honeypots
Chapter 13: Hacking Web Servers
Chapter 14: Hacking Web Applications
Chapter 15: SQL Injection
Chapter 16: Hacking Wireless Networks
Chapter 17: Hacking Mobile Platforms
Chapter 18: IoT Hacking
Chapter 19: Cloud Computing
Chapter 20: Cryptography

Included

40 hours of instructor-led training sessions
20 hands-on lab modules using industry tools
EC-Council authorized textbook/class materials