Certified Ethical Hacker (CEH)

Summary:

The Certified Ethical Hacker (CEH) program is the most comprehensive ethical hacking course on the globe to help information security professionals grasp the fundamentals of ethical hacking. It trains on the latest commercial-grade hacking tools, techniques, and methodologies used by hackers and information security professionals to lawfully hack an organization.

Prerequisites

- Minimum two years of work experience in information security domain
- Basic knowledge of networking and operating systems
- Understanding of TCP/IP protocols

Tools and Technologies

Nmap Wireshark Metasploit Burp Suite OWASP ZAP John the Ripper Hash cat

Why Choose This Course

- EC-Council Accredited Training Center with certified instructors
- Hands-on lab exercises covering over 220 attack technologies
- Access to the latest hacking tools and vulnerability exploitation techniques
- Real-world scenarios and practical applications of ethical hacking methodologies
- Compliance with international standards and best practices in cybersecurity
- Career support for security analyst and penetration tester roles
- Networking opportunities with cybersecurity professionals

Career Opportunities

- Ethical Hacker / Penetration Tester
- Security Analyst / Security Consultant
- Vulnerability Assessment Professional
- Network Security Specialist
- Security Operations Center (SOC) Analyst

- Information Security Manager
- Cybersecurity Consultant

Course Curriculum

Module 1: Introduction to Ethical Hacking

- Information Security Fundamentals
- Ethical Hacking Methodology
- Information Security Laws and Standards

Module 2: Foot-printing and Reconnaissance

- Foot-printing Tools and Techniques
- Foot-printing through Search Engines
- Foot-printing through Social Networking Sites
- Website Foot-printing and Competitive Intelligence

Module 3: Scanning Networks

- Network Scanning Methodologies
- TCP/IP Port and Service Scanning
- Host Discovery and OS Fingerprinting
- Firewall, IDS, and Honeypot Evasion

Module 4: Enumeration and Vulnerability Analysis

- Enumeration Concepts and Techniques
- SNMP, LDAP and NTP Enumeration
- Vulnerability Scanning Process
- Vulnerability Management Lifecycle

Module 5: System Hacking

- Password Cracking Techniques and Tools
- Privilege Escalation and Maintaining Access
- Buffer Overflows and Exploits
- Hiding Files and Covering Tracks

Module 6: Malware and Ransomware Operations

- Malware Types and Analysis
- Trojans, Viruses, and Worms
- Ransomware Techniques and Prevention
- Anti-Malware Countermeasures

Module 7: Sniffing and Social Engineering

- Packet Sniffing Techniques
- ARP Poisoning and MITM Attacks
- Social Engineering Techniques
- Identity Theft and Social Engineering Countermeasures

Module 8: Wireless, Mobile, and IoT Security

- Wireless Network Attacks
- Wireless Encryption Cracking
- Mobile Platform Attack Vectors
- IoT and OT Hacking

Module 9: Web Application Security

- Web Server Attacks
- Web Application Vulnerabilities
- SQL Injection Techniques

- Cross-Site Scripting and CSRF

Module 10: Cloud Computing and Cryptography

- Cloud Computing Threats
- Container Security
- Cryptographic Attacks
- Encryption Techniques and PKI

Course Features

Hands-on Labs

Certification Prep

Live Projects

Duration: 5 Weeks

Level: Intermediate

Certification

Upon course completion, participants will be prepared to take the EC-Council Certified Ethical Hacker (CEH) exam. The certification is valid for 3 years and can be renewed through EC-Council's Continuing Education program.

Certification Benefits

- Industry-recognized credential
- Enhanced job opportunities and career growth
- Validation of specialized skills and knowledge
- Increased earning potential
- Demonstrates commitment to professional development

Yes-M Systems

Instructor Profile

NAVEENKUMARYADAV LOYA

M.Tech in Computer Networks and Information Security, EC-Council Certified Instructor (CEI), CEH, CSA, CompTIA Security+

10+ years in cybersecurity, Linux, and networking

Professional Certifications

- EC-Council Certified Instructor (CEI)
- Certified Ethical Hacker (CEH)
- Certified Security Analyst (CSA)
- CompTIA Security+
- M.Tech in Computer Networks and Information Security

Experience Highlights

- 10+ years in cybersecurity & IT training
- CompTIA Instructor Network (CIN) member
- EC-Council Accredited Trainer
- SOC/NOC/IR team experience
- Trained 1000+ cybersecurity professionals

Frequently Asked Questions

What is the difference between a hacker and an ethical hacker?

While both possess similar technical skills, the key difference lies in permission and intent. Ethical hackers (also called 'white hat' hackers) operate with explicit permission from system owners, follow a strict code of ethics, and work to improve security. Traditional hackers ('black hat') operate without permission and often with malicious intent.

Will I be doing actual hacking during the course?

Yes, but in a legal and controlled environment. You'll work in isolated lab environments specifically designed for training purposes where you can practice ethical hacking techniques without legal concerns. All activities are supervised and comply with educational guidelines.

Is CEH recognized globally?

Yes, CEH is one of the most globally recognized ethical hacking certifications. It is accredited by ANSI and complies with the US Department of Defense Directive 8570. Many organizations worldwide require or prefer CEH certification for cybersecurity positions.

Can I legally perform penetration testing after getting CEH certified?

Certification alone doesn't grant legal permission to test systems. You must always obtain explicit written permission from the system owner before conducting any security assessment. The CEH certification demonstrates your competency but doesn't override legal requirements.

How often is the CEH curriculum updated?

EC-Council regularly updates the CEH curriculum to keep pace with evolving threats and technologies. Major version updates typically occur every 2-3 years, with minor updates more frequently. Our course always covers the latest CEH version and includes supplementary material on emerging threats.