Certified Ethical Hacker (CEH)

Certified Ethical Hacker (CEH) is a credential that equips you with essential skills to understand and counteract hackers by thinking like one, focusing on network security and ethical hacking techniques.

SEC-200

Course Outcomes

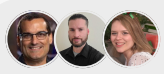
Professional, practical, & hands-on live instructor-led training

Further your skills and graduate as a certified professional, with the skills, experience, and job-search know how to get your career started.

Start Today

Potential Career Tracks

Ethical Hacker | Information Security Analyst | Network Security Professional | Penetration Tester | Cybersecurity Consultant | Security Specialist



Taught by Industry Veterans &
World Class Instructors

Introduction to Certified Ethical Hacker (CEH)

Course Overview

Intellectual Point's Certified Ethical Hacker (CEH) Training Course provides learners with the critical skills and knowledge needed to excel in the niche field of cybersecurity. This course is designed to teach you the practical aspects of ethical hacking through hands-on labs, real-world scenarios, and in-depth security protocols. It aims to prepare you for the CEH certification, ensuring you have a strong foundation in identifying vulnerabilities, system threats, and implementing defensive strategies. .

Throughout the training, you will explore the various phases of ethical hacking, starting with reconnaissance, gaining and maintaining access, and followed by covering tracks. You will delve deep into the latest tools and techniques used by both ethical hackers and malicious attackers. By the end of the course, you will be adept at identifying potential security risks, fortifying network infrastructures, and conducting vulnerability assessments.

Obtainable Skills

Vulnerability Assessment | Familiarity with Hacking Tools and Techniques | Exploit Detection | Network Defense and Security Protocols | Vulnerability Analysis | Risk Assessment and Mitigation | Network Security Configuration | Threat Analysis and Mitigation | Certification Exam Preparation

Course Insights

Audience Profile

The CEH Training Course is tailored for IT professionals with a keen interest in cybersecurity and a desire to understand the mindset and techniques of hackers. This course targets information security analysts, network security professionals, and system administrators who wish to fortify their understanding of security measures and protocols. It's also ideal for aspiring ethical hackers, security consultants, and anyone aiming to pursue a career in countering cyber threats and protecting valuable data assets. Previous experience in IT or related fields is beneficial, but not required, as the course offers foundational to advanced concepts.

Course Outcomes

By the end of this course, participants will:

1. Develop expertise in ethical hacking methodologies and penetrate testing techniques.
2. Identify and mitigate vulnerabilities in computer systems and networks effectively.
3. Perform comprehensive vulnerability assessments and implement strategic security defenses.
4. Understand and counteract techniques used by attackers to compromise systems.
5. Prepare for and achieve the Certified Ethical Hacker certification, advancing your career in cyber.

Module by Module Learning *Outline*

6 Modules

Module 1: Introduction to Ethical Hacking

Learning Objectives:

- Understand the role and importance of ethical hacking in cybersecurity.
- Differentiate between ethical hacking and malicious hacking.

Topics Covered

Ethical Hacking Fundamentals:

- Definition and scope of ethical hacking.
- Legal implications and ethical guidelines.

Cybersecurity Landscape:

- Overview of common cyber threats and vulnerabilities.
- Importance of staying updated with the latest security trends.

Module 2: Reconnaissance Techniques

Learning Objectives:

- Learn various tools and techniques for information gathering.
- Understand the first phase of ethical hacking: reconnaissance.

Topics Covered

Passive and Active Reconnaissance

- Differences between passive and active reconnaissance.
- Tools for effective information gathering.

Social Engineering:

- Identifying human factor vulnerabilities.
- Techniques for successful social engineering attacks.

Module 3: Scanning Networks

Learning Objectives:

- Master network scanning methodologies to identify system loopholes.
- Gain familiarity with scanning tools and techniques.

Topics Covered

Network Scanning Tools:

- Overview of popular scanning tools.
- Practical implementation of scanning methods.

Scanning Techniques:

- Types of scans: ping, port, and vulnerability scanning.
- Analyzing scanning results to assess risks.

Module 4: Gaining Access

Learning Objectives:

- Understand different methods of gaining unauthorized access to systems.
- Learn how to exploit system vulnerabilities.

Topics Covered

System Hacking Concepts:

- Identifying and exploiting system vulnerabilities.
- Techniques for password cracking and privilege escalation.

Malware Threats:

- Introduction to malware types and characteristics.
- Methods for detecting and preventing malware attacks.

Module 5: Maintaining Access and Covering Tracks

Learning Objectives:

- Learn methods used to maintain access to compromised systems.
- Understand techniques for erasing tracks to avoid detection.

Topics Covered

Persistent Threats:

- Methods for maintaining long-term access to networks.
- Use of backdoors and root-kits.

Covering Tracks:

- Techniques for hiding activities and avoiding detection.
- Ensuring traces of hacking activities are removed.

Module 6: Vulnerability Assessment and Security Measures

Learning Objectives:

- Conduct comprehensive vulnerability assessments.
- Implement defensive strategies to protect network infrastructures.

Topics Covered

Vulnerability Analysis:

- Tools and techniques for effective vulnerability scanning.
- Analyzing and interpreting vulnerability scan results.

Defensive Security Techniques:

- Strategies for implementing robust security protocols.
- Importance of regular security updates and patch management.