CEH – Ethical Hacker

Description

The CEH – Certified Ethical Hacker certification validates the knowledge and skills of individuals in the field of ethical hacking and penetration testing.

The main objective of the CEH certification is to train individuals to understand and think like a hacker in order to identify and exploit vulnerabilities and weaknesses in computer systems and networks. However, the purpose of ethical hacking is to perform these activities in a legal and responsible manner, with the explicit permission of the system owners, to help improve the security posture of organizations.

CEH certification is an important validation document for professionals who want to gain expertise in computer security. Certificate holders learn the tools and techniques used to test computer systems in a legal context, identify vulnerabilities and repair vulnerabilities. CEH training and certification is valuable to professionals working in the field of computer security and is a qualification sought after by many employers. Having this certification proves your ability to use ethical hacker techniques to detect and fix security vulnerabilities.

The Certified Ethical Hacker training can be attended by personnel who want to work in the network or information security department in institutions and gain a hacker perspective, or those who want to become a security penetration tester. This training also prepares you for the EC-Council Certified Ethical Hacker 312-50 exam.

What You Will learn

- Footprinting
- Network scanning
- Enumeration
- Packet sniffing
- Social Engineering

- DoS/DDoS
- Session hijacking
- Webserver and web application attacks and countermeasures
- SQL injection attacks
- Wireless encryption
- Cloud computing threats
- Cryptography ciphers
- Penetration testing

Who Should Attend

- Security officers

- Auditors

- Security professionals

- Site administrators

- Penetration testers

- Individuals concerned about the integrity of the network infrastructure

Outline

- Introduction to Ethical Hacking
- Footprinting and Reconaissance
- Scanning Networks
- Enumeration and Vulnerability Analysis
- System Hacking
- Malware Threats

- Sniffing
- Social Engineering
- Session Hijaking
- Evading IDS, Firewall and Honeypots
- Hacking Web Servers and Web Applications
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing

Prerequisites

A strong working knowledge of TCP/IP