AVWSQ-CEH

WSQ - Certified Ethical Hacker

5 Days Course • Instructor-Led Training (English)

About The Course

This five-day course focuses on hacking techniques and technologies from an offensive perspective. This advanced security program is regularly updated to reflect the latest developments in the domain, including new hacking techniques, exploits, automated programs as well as defensive recommendations as outlined by experts in the field. The CEH body of knowledge represents detailed contributions from security experts, academicians, industry practitioners and the security community at large.

Audience Profile

The Certified Ethical Hacking training course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Course Outcome

- Techniques and tools malicious hackers use, but in a lawful and legitimate manner
- Hacking into networks, systems, and web applications, with a goal to assess the potential impact and risk of an actual cyberattack, and to deploy necessary countermeasures
- Principles of ethical hacking, penetration testing methodology, reconnaissance of IT infrastructure, scanning for network, systems, and web application vulnerabilities
- Developing attack vectors to exploit the vulnerabilities
- Countermeasures to mitigate the risks of exploitation
- To assess and improve the security posture of a company's systems, network, and web applications
- Knowledge and skills needed to prepare for EC-Council's Certified Ethical Hacker (CEH) certification exam.

Pre-Requisites

It is recommended that participants have experience with Networking, Microsoft Server Management, Linux enterprise system, Web application development and Database administration.

WSQ Assessment Details

Participants are required to sit for an assessment on the last day of the course, which comprises of both written and practical assessment.

Course Outline

20 Modules

Module 1: Introduction to Ethical Hacking

Module 2: Footprinting and Reconnaissance

Module 3: Scanning Networks

Module 4: Enumeration

Module 5: Vulnerability Analysis

Module 6: System Hacking

Module 7: Malware Threats

Module 8: Sniffing

Module 9: Social Engineering

Module 10: Denial-of-Service

Module 11: Session Hijacking

Module 12: Evading IDS, Firewalls, and Honeypots

Module 13: Hacking Web Servers

Module 14: Hacking Web Applications

Module 15: SQL Injection

Module 16: Hacking Wireless Networks

Module 17: Hacking Mobile Platforms

Module 18: IoT Hacking

Module 19: Cloud Computing

Module 20: Cryptography