EC-Council - Certified Ethical Hacker v11

Code:	3617
Length:	5 days
URL:	View Online

The goal of this course is to help you master an ethical hacking methodology that can be used in penetration testing to lawfully assess the security of a system. This course delivers in-demand ethical hacking skills while preparing you for the internationally-recognized Certified Ethical Hacker certification exam (312-50) from EC-Council.

EC Council security experts have designed over 140 labs, which mimic real-time scenarios to help you “live” through an attack as if it were real. You’ll also be given access to over 2,200 commonly used hacking tools to immerse you into the hacker world.

Why take Certified Ethical Hacker?

Given the many cybersecurity attacks and great volume of personal data at risk, plus the potential legal liabilities, the need for certified ethical hackers is quite high. This course is a must-take for anyone responsible for network and data security who is looking to get CEH certified.

CEH Exam Voucher INCLUDED This course includes one exam voucher for the CEH - Certified Ethical Hacker v11 exam (312-50).

Skills Gained

- Footprinting
- Network scanning
- Enumeration
- Packet sniffing
- Social Engineering
- DoS/DDoS attacks
- Session hijacking
- Webserver and web application attacks and countermeasures
- SQL injection attacks
- Wireless encryption
- Cloud computing threats
- Cryptography ciphers
- Penetration testing
- Hacking challenges on steroids
- Emerging attack vectors
- Malware reverse engineering
- Operation technology
- WPA3

Who Can Benefit

- Security officers
- Auditors
- Security professionals
- Site administrators
- Penetration testers
- Individuals concerned about the integrity of network infrastructure

Prerequisites

- At least two years of IT security experience
- A strong working knowledge of TCP/IP

Course Details

Topics

- Module 01: Introduction to Ethical Hacking
- Module 02: Footprinting and Reconnaissance
- Module 03: Scanning Networks
- Module 04: Enumeration
- Module 05: Vulnerability Analysis
- Module 06: System Hacking
- Module 07: Malware Threats
- Module 08: Sniffing
- Module 09: 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
