Certified Ethical Hacker (C|EH)

Course Description

C|EH is the world's most advanced certified ethical hacking course that covers 20 of the most current security domains any individual will ever want to know when they are planning to beef-up the information security posture of their organization.

The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals.

Key Outcomes

- Thorough introduction to ethical hacking
- Exposure to threat vectors and countermeasures
- Addresses emerging areas of IoT, cloud and mobile hacking
- Prepares you to combat Trojans, malware, backdoors, and more
- Enables you to hack using mobile

Exam Information

- Exam Title: Certified Ethical Hacker (ANSI)
- Exam Code: 312-50 (ECC EXAM), 312-50 (VUE)
- Number of Questions: 125
- Duration: 4 hours
- Availability: ECC Exam Portal, VUE
- Test Format: Multiple Choice
- Passing Score: Please refer to https://cert.eccouncil.org/faq.html

Course Outline

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography