Certified Ethical Hacker

Duration

5 Days

Introduction

CEH provides a comprehensive **ethical hacking and network security-training program** to meet the standards of highly skilled security professionals. Hundreds of SMEs and authors have contributed towards the content presented in the CEH courseware. Latest tools and exploits uncovered from the underground community are featured in the new package. Our researchers have invested thousands of man hours researching the latest trends and uncovering the covert techniques used by the underground community.

Audience

- Security officers
- Auditors
- Security professionals
- Site administrators, and
- Anyone who is concerned about the integrity of the network infrastructure

Course Objective

This class will immerse the students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a student leaves this intensive 5 day class they will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council Certified Ethical Hacker exam

Course Topics

1. **Introduction to Ethical Hacking**
2. **Foot printing and Reconnaissance**
3. **Scanning Networks**
4. **Enumeration**
5. **System Hacking**
6. **Trojans and Backdoors**
7. **Viruses and Worms**
8. **Sniffers**
9. **Social Engineering**
10. **Denial of Service**
11. **Session Hijacking**
12. **Hacking Web servers**
13. **Hacking Web Applications**
14. **SQL Injection**
15. **Hacking Wireless Networks**
16. **Evading IDS, Firewalls and Honeypots**
17. **Buffer Overflows**

18. **Cryptography**
19. **Penetration Testing**

Exam Format

- Number of Questions: 125
- Passing Score: 70%
- Test Duration: 4 Hours
- Test Format: Multiple Choice
- Test Delivery: Prime Prometric (IBT), VUE, and APTC
- Exam Prefix: 312-50-ANSI (IBT), 312-50v9 (VUE), or 350 CEHv9 (APTC)