Ethical Hacking & Countermeasures Certification CEH V7

CERTIFICATION
Training Description

This Training will immerse the candidate 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 candidate in-depth knowledge and practical experience with the current essential security systems. Candidate will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks, no real network is harmed. Candidate then learn how intruders escalate privileges and what steps can be taken to secure a system. Candidate will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. When a candidate leaves after this intensive class they will have hands on understanding and experience in Ethical Hacking. This course prepares you for EC-Council Certified Ethical Hacker exam 312-50.

Who Should Attend:
This course will significantly benefit to CIO, CTO, Chief Information Security Officers, Software & System Engineers , IT Managers & Head's, Security auditors, Security & Networking professionals, Site administrators, Secure Programmers and developers, Database Administrators and anyone who is concerned about the integrity of the network infrastructure security.

Duration Options
5 Days
15 Days
1 Months
3 Months

Certification
The Certified Ethical Hacker exam 312-50 may be taken on the last day of the training (optional). Candidate need to pass the online Prometric exam to receive CEH certification.

Mirox also provide special Corporate Information Security Training for Banking, Insurance, Healthcare, Research centers, Pharmaceutical Industries, Retail marketing, IT companies, Education centers & Universities, Insurance, Telecommunications Manufacturing Industries and various Government organizations etc

Some of the hacking concepts you will learn to master during this hands on hacking course

Module 01: Introduction to Ethical Hacking

Module 02: Footprinting and Reconnaissance

Module 03: Scanning Networks

Module 04: Enumeration

Module 05: System Hacking

Module 06: Trojans and Backdoors

Module 07: Viruses and Worms

Module 08: Sniffers

Module 09: Social Engineering

Module 10: Denial of Service

Module 11: Session Hijacking

Module 12: Hacking Webservers

Module 13: Hacking Web Applications

Module 14: SQL Injection

Module 15: Hacking Wireless Networks

Module 16: Evading IDS, Firewalls, and Honeypots

Module 17: Buffer Overflow

Module 18: Cryptography

Module 19: Penetration Testing