

C)PEH: Certified Professional Ethical Hacker

Course ID #: 7000-809-ZZ-Z

Hours: 35

Course Content

Course Description:

In this course, you will learn the value of vulnerability assessments. Then, you will discover how to use those assessments to make powerful changes in an information system's security. Additionally, you will learn how malware and destructive viruses function and how to implement counter response and preventative measures when it comes to a network hack.

Course Objectives:

Upon successful completion of this course students will be able to competently take the C)PEH exam.

Prerequisites:

- C)SP
- 12 months of IT Experience
- 12 Months of Networking Experience

Target Audience:

- IS Security Owners
- Security Officers
- Ethical Hackers
- Information Owners
- Penetration Testers
- System Owners and Managers
- Cyber Security Engineers

Topics:

Lesson 1 – Introduction to Ethical Hacking

- What and Why?
- Differences
- Security Definitions
- Risk Management
- Methodologies

Lesson 2 – Linux Fundamentals

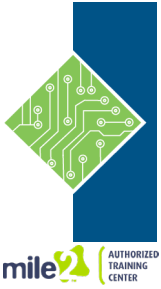
- Core Concepts
- The shell and other items you need to know
- Managing users
- Basic Commands

Lesson 3 – Protocols

- Network Models
- Protocols & Services

Lesson 4 – Cryptography

- Understanding Cryptography
- Symmetric Encryption
- Asymmetric Encryption
- Hashing
- Cryptography in Use
- Crypto Attacks



C)PEH: Certified Professional Ethical Hacker

Course ID #: 7000-809-ZZ-Z

Hours: 35

Lesson 5 – Password Cracking

- What and Why
- Attacks and Tools of the Trade
- Countermeasures

Lesson 6 – Malware

- DOS & DDOS
- Viruses & Backdoors
- Trojans and Backdoors
- Ransomware

Lesson 7 – Security Devices

- Basic Security Elements
- Security Appliances

Lesson 8 – Information Gathering

- What are we looking for?
- Where/How do we find this information?
- Are there tools to help?

Lesson 9 – Social Engineering

- Social Engineering Types
- Phishing Scams

Lesson 10 – Reconnaissance

- What are we looking for?
- Port Scanning
- Are there tools to help?
- Banner Grabbing
- Enumeration

Lesson 11 – Vulnerability Assessment

- What is a Vulnerability Assessment
- Tools of the Trade
- Testing Internal and External Systems

Lesson 12 - Network Attacks

- Sniffing Techniques
- Hijacking

Lesson 13 – Hacking Servers

- Servers, What are they good for?
- What is an Exploit?
- Tools of the Trade

Lesson 14 – Hacking Web Technologies

- OWASP Top 10
- SQL Injection
- XSS

Lesson 15 – Hacking Wireless Networks

- Wireless Technologies
- Mobile and IoT Technologies
- Various Tools Used
- Hacking Techniques
- Countermeasures



C)PEH: Certified Professional Ethical Hacker

Course ID #: 7000-809-ZZ-Z

Hours: 35

Lesson 16 – Maintaining Access and Covering Tracks

- Maintaining Access
- Covering Tracks

Labs:

- Lab 1 – Intro to C)PEH Setup
- Lab 2 - Linux Fundamentals
- Lab 3 – Understanding Protocols
- Lab 4 - Cryptography Lab
- Lab 5 – Password Cracking
- Lab 6 - Malware
- Lab 7 – Information Gathering
- Lab 8 – Information Gathering – Active Reconnaissance
- Lab 9 – Vulnerability Assessment
- Lab 10 – Network Sniffing/IDS
- Lab 11 - Windows Hacking
- Lab 12 – Attacking Databases
- Lab 13 – Attacking Web Applications
- Lab 14 - Backdoors

Accreditations:



Register for this class by visiting us at:

www.tcworkshop.com or calling us at 800-639-3535