CPEH
Certified Professional Ethical Hacker

Overview

The Certified Professional Ethical Hacker vendor-neutral certification course is the foundational training to Mile2's line of penetration testing courses.

The CPEH certification training enables students to understand the importance of vulnerability assessments by providing industry knowledge and skills in Vulnerability Assessments. In doing so, the CPEH student is able to understand how malware and destructive viruses function. In addition, the CPEH course helps students learn how to implement counter response and preventative measures when it comes to a network hack.

Accreditation & Acknowledgements

ACCREDITED by the NSA CNSS 4011-4016
MAPPED to NIST / Homeland Security NICCS's Cyber Security Workforce Framework
APPROVED on the FBI Cyber Security Certification Requirement list (Tier 1-3)

Upon Completion

Upon completion, the Certified Professional Ethical Hacker candidate will be able to competently take the CPEH exam.

Course Length

5 days

Format

- Instructor-led classroom
- Live Online Training

Prerequisites

- 12 months of IT security experience
- 12 months of Networking Experience

Student Materials

- Student Workbook
- Student Lab guide
- Exam Prep Guide
- CPEs: 40

Certification Exam

The Certified Professional Ethical Hacker exam is taken online through Mile2’s Assessment and Certification System (“MACS”), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple-choice questions.

Who Should Attend?

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

Course Contents

- Module 0 - Course Introduction
- Module 1 – Introduction to Ethical Hacking
- Module 2 - Linux Fundamentals
- Module 3 - Protocols
- Module 4 - Cryptography
- Module 5 - Password Cracking
- Module 6 - Malware
- Module 7 - Security Devices
- Module 8 - Information Gathering - Passive Reconnaissance
- Module 9 - Social Engineering
- Module 10 - Active Reconnaissance

- Module 11 - Vulnerability Assessment
- Module 12 - Network Attacks
- Module 13 - Hacking Servers
- Module 14 - Hacking Web Technologies
- Module 15 - Hacking Wireless Technologies
- Module 16 - Maintaining Access and Covering Tracks

Lab Outline

- 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 - Vulnerability Assessment
- Lab 9 - Network Sniffing / IDS
- Lab 10 - Windows Hacking
- Lab 11 - Attacking Databases
- Lab 12 - Attacking Web Applications
- Lab 13 - Backdoors