Certified Professional Ethical Hacker "CPEH"

Course Title:

Certified Professional Ethical Hacker - CPEH

Duration:

5 days, 40 Hours

Class Format Options:

Instructor-led classroom

Who Should Attend:

- *Incident Handlers*
- *SOC operators*
- *Security Consultants*
- *Ethical Hackers*
- *IT Management*
- *Chief Security Officers*

Prerequisites:

An Interest in penetration testing and ethical hacking

Advanced Related Courses:

- *C)PTE: Penetration Testing Engineer*
- *C)PTC: Penetration Testing Consultant*

Course Overview

The Certified Professional Ethical Hacker course is the introductory training to mile2's line of penetration testing courses and certifications. The course training helps students gain a valuable skillset in penetration testing by understand the importance of vulnerability assessments and ethical hacking through:

- Learning the knowledge and skills behind a vulnerability assessment.
- Preparation to apply this knowledge and exercise these skills in the interest of others.
- Understand the importance of a Vulnerability Assessment and how it can help you prevent serious break-ins to your organization.

This is accomplished by:

- Performing in-depth labs with industry standard tools.
- Learning the penetration testing methodology through conceptual theories and real-world practices.
- Equipping you with the knowledge about what hackers look for when trying to hack into your network.
- Assessing for the cause of testing your company's security posture to help better

Upon Completion

Students will:

- Have knowledge to perform ethical hacking for vulnerability assessments.
- Have knowledge to accurately report on their findings.
- Be ready to sit for the C)PEH exam.

Exam Information:

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 C)PEH exam will take 2 hours and consist of 100 multiple choice questions.

Contact: info@cyberm.co.za / +27 83 262 2025

Certified Professional Ethical Hacker - CPEH: Course Content

Module 1: Security Fundamentals

Module 2: Access Controls

Module 3: Protocols

Module 4: Cryptography

Module 5: Why Vulnerability Assessments

Module 6: Vulnerability Tools of the Trade

Module 7: Output Analysis and Reports

Module 8: Reconnaissance, Enumeration

Module 9: Gaining Access

Module 10: Maintaining Access

Module 11: Covering Tracks

Module 12: Malware

Module 13: Buffer Overflows

Module 14: Password Cracking

Appendix 1 - Economics and Law

Appendix 2 - Vulnerability Types

Appendix 3 - Assessing Web Servers

Appendix 4 - Assessing Remote & VP Services

Appendix 5 - Denial of Service

Review and (Exam if applicable)

Lab Objectives:

This is an intensive, hands-on class. And as such, our focus will be on the ethical hacking model of penetration testing. Students will work through mile2's intensive proprietary labs in our cyber range learning structured attacks and counter controls in both Windows and Linux systems.

These labs will provide students with the experience necessary to perform ethical hacking on their own business and to recommend solutions to vulnerabilities found.