Certified Penetration Testing Engineer "CPTE"

Course Title:

Certified Penetration Testing Engineer - CPTE

Duration:

5 days, 40 Hours

Class Format Options:

Instructor-led classroom
Live Virtual Training
Computer Based Training

Who Should Attend:

IT Auditors
System Administrators
IS Managers

Prerequisites:

A minimum of 12 months networking technologies experience.
Sound knowledge of TCP/ IP Network+, Security+
Basic Knowledge of Linux

Provided Materials:

Student Workbook Student Reference Manual Student Lab Guide Software/Tools (DVDs)

Certification Track:

C)PTE - Certified Penetration Testing Engineer
C)PTC - Certified Penetration Testing Consultant

Certification Exam:

C)PTE - Certified Penetration Testing Engineer

Course Overview

The Certified Penetration Testing Engineer course trains students on the 5 key elements of penetration testing:

1. Information Gathering
2. Scanning
3. Enumeration
4. Exploitation
5. Reporting

Ethical hacking is the art of using these penetration-testing techniques to identify and repair the latest vulnerabilities in a system to make sure it is secure. Malicious hackers use these same techniques to find the same vulnerabilities except they exploit the vulnerabilities giving them access to the businesses' network. Once inside, hackers can access private information, such as usernames, passwords, credit card numbers, and social security numbers of clients and employees. It's very likely this data will be held for ransom or sold off on a black market. Hackers are constantly looking for new companies they can exploit; when they come across yours, will they be able to gain access? Certified Penetration Testing Engineers are the solution to prevent this from happening to businesses they serve.

This course also enhances the business skills needed to identify protection opportunities, justify testing activities and optimize security controls appropriate to the business needs in order to reduce business risk. The C)PTE's foundation is built firmly upon proven, hands-on, penetration testing methodologies utilized by our international group of vulnerability consultants. Mile2 trainers keep abreast of their field by practicing what they teach; we believe that an equal emphasis on theoretical and real world experience is essential for effective knowledge transfer to you, the student.

Upon Completion

Students will:

- Have knowledge to perform penetration test
- Have knowledge to accurately report on their findings from examinations
- Be ready to sit for the C)PTE Exam (if applicable).
  Exam Information: The Certified Penetration Testing Engineer 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.

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

Certified Penetration Testing Engineer CPTE: Course Content

Module 0: Course Overview

Module 1: Logistics of Pen Testing

Module 2: Linux Fundamentals

Module 3: Information Gathering

Module 4: Detecting Live Systems

Module 5: Enumeration

Module 6: Vulnerability Assessments

Module 7: Malware Goes Undercover

Module 8: Windows Hacking

Module 9: Hacking UNIX/Linux

Module 10: Advanced Exploitation Techniques

Module 11: Pen Testing Wireless Networks

Module 12: Networks, Sniffing and IDS

Module 13: Injecting the Database

Module 14: Attacking Web Technologies

Module 15: Project Documentation

Lab 1: Getting Set Up

Lab 2: Linux Fundamentals

Lab 3: Information Gathering

Lab 4: Detecting Live Systems

Lab 5: Reconnaissance

Lab 6: Vulnerability Assessment

Lab 7: Malware

Lab 8: Windows Hacking

Lab 9: UNIX/Linux Hacking

Lab 10: Advanced Vulnerability and Exploitation

Lab 11: Attacking Wireless Networks

Lab 12: Network Sniffing and IDS

Lab 13: Database Hacking

Lab 14: Hacking Web Applications

Lab 15: Cryptography

Post Class Lab: Core Impact