CPTE
Certified Penetration Testing Engineer

Overview

The vendor-neutral Certified Penetration Testing Engineer certification course is built firmly upon proven, hands-on, Penetration Testing methodologies utilized by our international group of Penetration Testing Consultants.

The C)PTE presents information based on the 5 Key Elements of Pen Testing; Information Gathering, Scanning, Enumeration, Exploitation, and Reporting. The latest vulnerabilities will be discovered using these tried and true techniques.

Accreditation

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, Certified Penetration Testing Engineer students will be able to establish industry acceptable auditing standards with current best practices and policies. Students will also be prepared to competently take the C)PTE exam.

Course Length

5 days

Format

- Instructor-led classroom
- Computer Based Training
- CBT - Pre-recorded Videos

Prerequisites

- A minimum of 12 months' experience in networking technologies
- Sound knowledge of TCP/IP
- Knowledge of Microsoft packages
- Network+, Microsoft, Security+
- Basic Knowledge of Linux is essential

Student Materials

- Student Workbook
- Student Prep Guide

Certification Exam

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

Who Should Attend?

- Pen Testers
- Ethical Hackers
- Network Auditors
- Cyber Security Professionals
- Vulnerability Assessors
- Cyber Security Managers
- IS Managers

Course Contents

- **Module 0** - Course Introduction
- **Module 1** - Business & Technical Logistics of Pen Testing
- **Module 2** - Information Gathering Reconnaissance - Passive (External Only)
- **Module 3** - Detecting Live Systems – Reconnaissance (Active)
- **Module 4** - Banner Grabbing and Enumeration
- **Module 5** - Automated Vulnerability Assessment
- **Module 6** - Hacking Operating Systems

- **Module 7** - Advanced Assessment and Exploitation Techniques
- **Module 8** - Evasion Techniques
- **Module 9** - Hacking with PowerShell
- **Module 10** - Networks and Sniffing
- **Module 11** - Accessing and Hacking Web Techniques
- **Module 12** - Mobile and IoT Hacking
- **Module 13** - Report Writing Basics
- **Appendix:** Linux Fundamentals

Lab Outline

- **Lab 1** - Introduction to Pen Testing Setup
- **Lab 2** - Linux Fundamentals
- **Lab 3** - Using Tools For Reporting
- **Lab 4** - Information Gathering
- **Lab 5** - Detecting Live Systems - Scanning Techniques
- **Lab 6** - Enumeration
- **Lab 7** - Vulnerability Assessments
- **Lab 8** - Software Goes Undercover
- **Lab 9** - System Hacking - Windows
- **Lab 10** - System Hacking – Linux/Unix Hacking
- **Lab 11** - Advanced Vulnerability and Exploitation Techniques
- **Lab 12** - Network Sniffing/IDS
- **Lab 13** - Attacking Databases
- **Lab 14** - Attacking Web Applications