Certified Penetration Testing Engineer

KEY DATA

Course Title: Certified Penetration Testing Engineer v5

Duration: 5 days

Language: English

Class Format Options:

- Instructor-led classroom
- Live Online 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 Lab Guide
- Prep Guide

Certification Exam:

CPTE – Certified Pen Testing Engineer™ (taken through mile2's MACS online testing system)

CPEs: 40

Who Should Attend:

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

COURSE 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.

This course also enhances the business skills needed to identify protection opportunities, justify testing activities and optimize security controls to reduce risk associated to working with the internet. The student will be using the latest tools, such as **Saint**, **Metasploit** through **Kali Linux** and **Microsoft PowerShell**.

Mile2 goes far beyond simply teaching you to "Hack". The C)PTE was developed around principles and behaviors used to combat malicious hackers and focuses on professional penetration testing rather than "ethical hacking".

Besides utilizing ethical hacking methodologies, the student should be prepared to learn penetration testing methodologies using advanced persistent threat techniques. In this course, you will go through a complete penetration test from A-Z! **You'll learn to create your own assessment report and apply your knowledge immediately in the work force**.

With this in mind, the CPTE certification course is a complete up-grade to the EC-Council CEH! The C)PTE exam is taken any time/anywhere on-line through mile2's MACS system, making the exam experience easy and mobile. Student does not need to take the C)PTE course to attempt the C)PTE exam.

Pen Testing Hacking Career

C)VA™ Certified Vulnerability Assessor

C)PEH™ CERTIFIED PROFESSIONAL ETHICAL HACKER

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER *

C)PTC™ CERTIFIED PENETRATION TESTING CONSULTANT

All Combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide)
- Exam Prep Guide
- Exam
- Cyber Range Lab

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

mile2® CYBER SECURITY CERTIFICATIONS

ACCREDITATIONS

COMMITTEE ON NATIONAL SECURITY SYSTEMS — CNSS — SYSTEMS SECURITY FOR THE 21st CENTURY

NICCS™ NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

DEPARTMENT OF JUSTICE — FEDERAL BUREAU OF INVESTIGATION — FIDELITY BRAVERY INTEGRITY

mile2 is **ACCREDITED** by the **NSA CNSS 4011-4016**
Is **MAPPED** to NIST/Homeland Security NICCS's Cyber Security Workforce Framework
is **APPROVED** on the **FBI Cyber Security Certification Requirement list (Tier 1-3)**

The Certified Penetration Testing Engineer course is accredited by the NSA CNSSI-4013: National Information Assurance Training.

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.

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. The cost is $400 USD and must be purchased from Mile2.com.

macs Assessment & Certification System

COURSE DETAILS

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

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

mile2® CYBER SECURITY CERTIFICATIONS

DETAILED HANDS-ON LABORATORY OUTLINE

Lab 1 – Introduction to Pen Testing Setup
Section 1 – Recording IPs and Logging into the VMs
Section 2 – Research

Lab 2 – Linux Fundamentals
Section 1 – Command Line Tips & Tricks
Section 2 - Linux Networking for Beginners
Section 3 – Using FTP during a pentest

Lab 3 – Using tools for reporting
Section 1 – Setting up and using magictree

Lab 4 – Information Gathering
Section 1 – Google Queries
Section 2 – Searching Pastebin
Section 3 – Maltego
Section 4 – People Search Using the Spokeo Online Tool
Section 5 – Recon with Firefox
Section 6 – Documentation

Lab 5 – Detecting Live Systems - Scanning Techniques
Section 1 – Finding a target using Ping utility
Section 2 – Footprinting a Target Using nslookup Tool
Section 3 – Scanning a Target Using nmap Tools
Section 4 – Scanning a Target Using Zenmap Tools
Section 5 – Scanning a Target Using hping3 Utility
Section 6 – Make use of the telnet utility to perform banner grabbing
Section 7 – Documentation

Lab 6 – Enumeration
Section 1 – OS Detection with Zenmap
Section 2 – Enumerating a local system with Hyena
Section 3 – Enumerating services with nmap
Section 4 – DNS Zone Transfer
Section 5 – LDAP Enumeration

Lab 7 – Vulnerability Assessments
Section 1 – Vulnerability Assessment with SAINT
Section 2 – Vulnerability Assessment with OpenVAS

Lab 8 – Software Goes Undercover
Section 1 – Creating a Virus

Lab 9 – System Hacking – Windows Hacking
Section 1 – System Monitoring and Surveillance
Section 2 – Hiding Files using NTFS Streams
Section 3 – Find Hidden ADS Files
Section 4 – Hiding Files with Stealth Tools
Section 5 – Extracting SAM Hashes for Password cracking
Section 6 – Creating Rainbow Tables
Section 7 – Password Cracking
Section 8 – Mimikatz

Lab 10 – System Hacking – Linux/Unix Hacking
Section 1 – Taking Advantage of Misconfigured Services
Section 2 – Cracking a Linux Password
Section 3 – Setting up a Backdoor

Lab 11 – Advanced Vulnerability and Exploitation Techniques
Section 1 – Metasploitable Fundamentals
Section 2 – Metasploit port and vulnerability scanning
Section 3 – Client-side attack with Metasploit
Section 4 – Armitage

Lab 12 – Network Sniffing/IDS
Section 1 – Sniffing Passwords with Wireshark
Section 2 – Performing MitM with Cain
Section 3 – Performing MitM with sslstrip

Lab 13 – Attacking Databases
Section 1 – Attacking MySQL Database
Section 2 – Manual SQL Injection

Lab 14 – Attacking Web Applications
Section 1 – Attacking with XSS
Section 2 – Attacking with CSRF

DETAILED COURSE OUTLINE

Module 0 – Course Introduction

Module 1 – Business and Technical Logistics of Pen Testing

- Section 1 – What is Penetration Testing?
- Section 2 – Today's Threats
- Section 3 – Staying up to Date
- Section 4 – Pen Testing Methodology
- Section 5 – Pre-Engagement Activities

Module 2 – Information Gathering Reconnaissance- Passive (External Only)

- Section 1 – What are we looking for?
- Section 2 – Keeping Track of what we find!
- Section 3 – Where/How do we find this Information?
- Section 4 – Are there tools to help?
- Section 5 - Countermeasures

Module 3 – Detecting Live Systems – Reconnaissance (Active)

- Section 1 – What are we looking for?
- Section 2 – Reaching Out!
- Section 3 – Port Scanning
- Section 4 – Are there tools to help?
- Section 5 - Countermeasure

Module 4 – Banner Grabbing and Enumeration

- Section 1 – Banner Grabbing
- Section 2 - Enumeration

Module 5 – Automated Vulnerability Assessment

- Section 1 – What is a Vulnerability Assessment?
- Section 2 – Tools of the Trade
- Section 3 – Testing Internal/External Systems
- Section 4 – Dealing with the Results

Module 6 – Hacking Operating Systems

- Section 1 – Key Loggers
- Section 2 - Password Attacks
- Section 3 – Rootkits & Their Friends
- Section 4 – Clearing Tracks

Module 7 – Advanced Assessment and Exploitation Techniques

- Section 1 – Buffer Overflow
- Section 2 - Exploits
- Section 3 – Exploit Framework

Module 8 – Evasion Techniques

- Section 1 – Evading Firewall
- Section 2 - Evading Honeypots
- Section 3 – Evading IDS

Module 9 – Hacking with PowerShell

- Section 1 – PowerShell – A Few Interesting Items
- Section 2 – Finding Passwords with PowerShell

Module 10 – Networks and Sniffing

- Section 1 - Sniffing Techniques

Module 11 – Accessing and Hacking Web Techniques

- Section 1 - OWASP Top 10
- Section 2 – SQL Injection
- Section 3 - XSS

Module 12 – Mobile and IoT Hacking

- Section 1 – What devices are we talking about?
- Section 2 – What is the risk?
- Section 3 – Potential Avenues to Attack
- Section 4 – Hardening Mobile/IoT Devices

Module 13 – Report Writing Basics

- Section 1 – Report Components
- Section 2 – Report Results Matrix
- Section 3 - Recommendations

Appendix – Linux Fundamentals

- Section 1 – Core Concepts
- Section 2 – The Shell and other items you need to know
- Section 3 – Managing Users
- Section 4 – Basic Commands