Certified Penetration Testing Engineer (CPTE)

Modality: Virtual Classroom

Duration: 5 Days

About the course:

The most recent vulnerabilities will be found utilizing these true and tried techniques. This course also upgrades the abilities of the business expected to recognize the opportunities for protection, optimize security controls and justify testing activities to diminish the hazard related to working with the web. The learner will utilize the most recent instruments, for example, Saint, Metasploit with Microsoft PowerShell and Kali Linux. Mile2 goes a long way past simply instructing you to "Hack". The CPTE was created around standards and practices used to battle malicious programmers and targets on proficient penetration testing as opposed to " ethical hacking ". Other than using the methodologies of ethical hacking, the learner must be ready to learn methodologies of penetration testing utilizing progressed persistent risk strategies. In this course, you will experience a total penetration test from A-Z! You'll figure out how to make your own evaluation report and apply your insight promptly in the workforce. In view of this, the certification course of CPTE is a finished move up to the EC-Council CEH! The exam of CPTE is taken anyplace/anytime online through mile2's MACS framework, making the test experience simple and versatile. The learner doesn't have to take the course of CPTE to endeavor the exam of CPTE.

Salary Estimate:

The normal pay for Certified Penetration Testing Engineer is $71,660 annually.

Course Objective:

In the wake of finishing this course, understudies will have the option to:

1. Have the information to precisely report their findings from assessments
2. Have the information to play out a penetration test
3. Be prepared to sit for the Exam of CPTE

Targeted Audience:

This course is planned for:

1. Pen Testers
2. Cyber Security Managers
3. Network Auditors
4. Ethical Hackers
5. IS Managers
6. Vulnerability Assessors
7. Cyber Security professionals

Prerequisites:

1. An experience of 12 months in networking technologies
2. Understanding of Microsoft packages
3. Comprehensive information of TCP/IP
4. Basic understanding of Linux is necessary
5. Network+, Security+, Microsoft

Recommended prerequisites courses:

- Exam N10-006 - CompTIA Network+
- Certification Boot Camp A+ Network+ and Security+ (COMP-A+NET+SEC+)

Course Outline:

- **Module 0** - Course Overview
- **Module 1** – Business & Technical 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
- **Module 16** - Securing Windows s/ Powershell
- **Module 17** - Pen Testing w/Powershell

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
- **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
- **Lab 12** - Network Sniffing/IDS
- **Lab 13** - Attacking Databases
- **Lab 14** - Attacking Web Applications