Document Generated: 12/18/2025

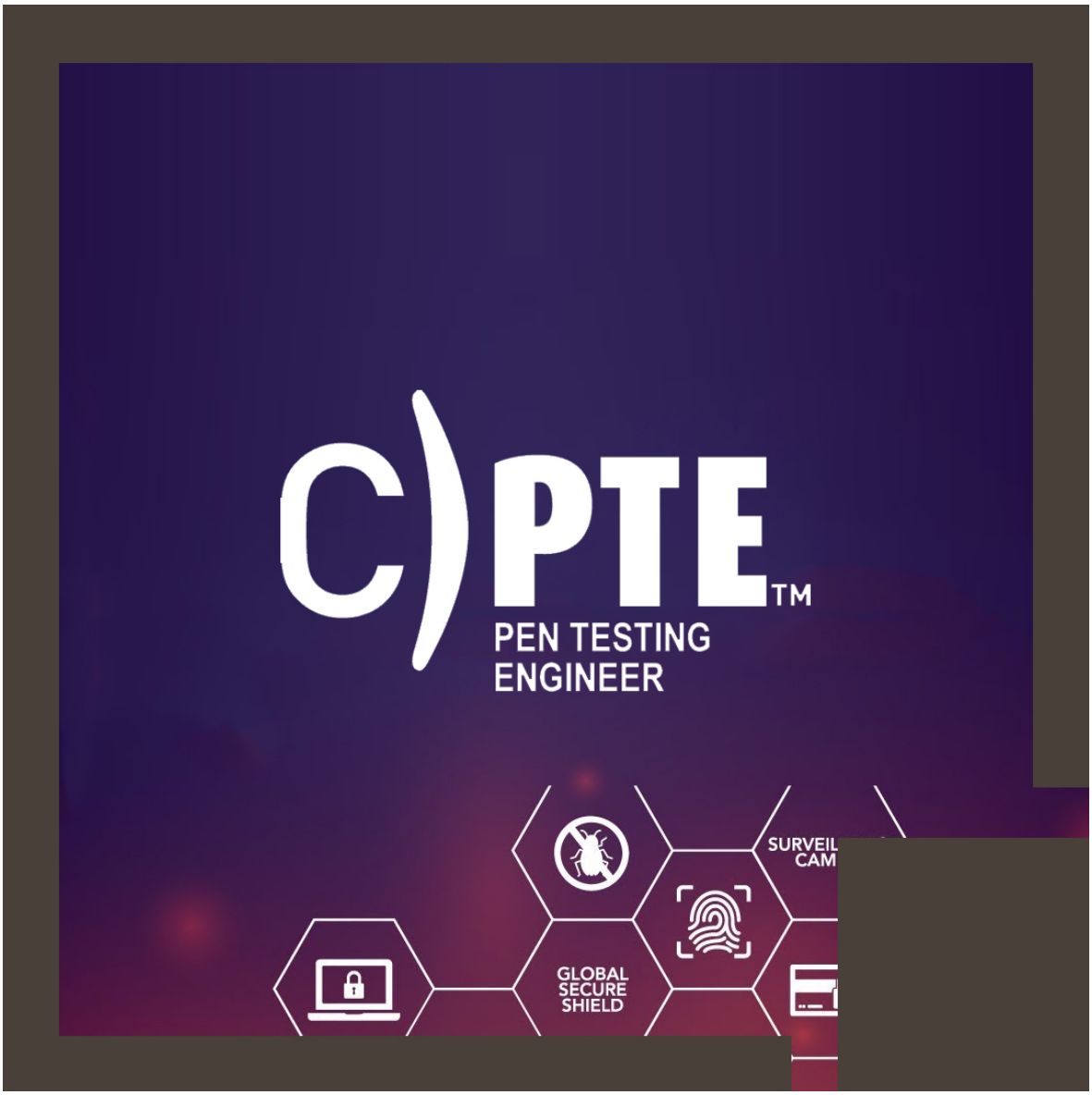
Learning Style: On Demand

Technology:

Difficulty: Intermediate

Course Duration: 7 Hours

Certified Penetration Testing Engineer



About this course:

A penetration test is an endeavor to assess the security of an IT foundation by securely attempting to abuse vulnerabilities. These vulnerabilities may present in working frameworks, application and services imperfections, inappropriate designs or unsafe end-client conduct. Also, such evaluations are valuable in approving the adequacy of cautious instruments and also end-user adherence to security approaches. This Official certification training series of Mile2® cybersecurity covers all that you have to think about turning into a Certified Penetration Testing Engineer. Understudies will find out about Linux fundamentals, logistics of pen testing, detecting live systems, information gathering, vulnerability assessments, enumeration, Windows hacking, malware going undercover, advanced exploitation techniques, hacking UNIX/Linux, networks, pen testing wireless networks, injecting the database, sniffing and IDS, project documentation, and attacking web technologies.

The normal pay for Certified Pen Tester is $71,660 every year.

Course Objective:

- Build up industry adequate evaluating standards with great procedures and arrangements
- Logistics of Pen Testing
- Vulnerability Assessments
- Information Gathering
- Linux Fundamentals
- Detecting Live Systems
- Enumeration
- Pen Testing Wireless Networks
- Malware Goes Undercover
- Hacking UNIX/Linux
- Windows Hacking
- Injecting the Database
- Advanced Exploitation Techniques
- Project Documentation
- Networks, Sniffing and IDS
- Attacking Web Technologies

Audience:

This course is designed for:

- Pen Testers
- Network Auditors
- Ethical Hackers
- Cyber Security Professionals

Prerequisites:

- Minimum experience of 12 months in networking technologies
- Basic information of Linux is essential
- Understanding of MS packages
- A sound information of TCP/IP
- Microsoft, Network+, Security+.

Course Outline:

This Course Includes:

- Course Introduction
- Module 1 - Business and Technical Logistics for Pen Testing
- Module 2 - Information Gathering - Reconnaissance Passive
- Module 3 - Detecting Live Systems - Reconnaissance-Active
- Module 4 - Banner Grabbing & 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, Sniffing, and IDS
- Module 11 - Assessing and Hacking Web Technologies
- Module 12 - Mobile and IoT Hacking
- Module 13 - Report Writing Basics
- Course Summary