Document Generated: 06/18/2025

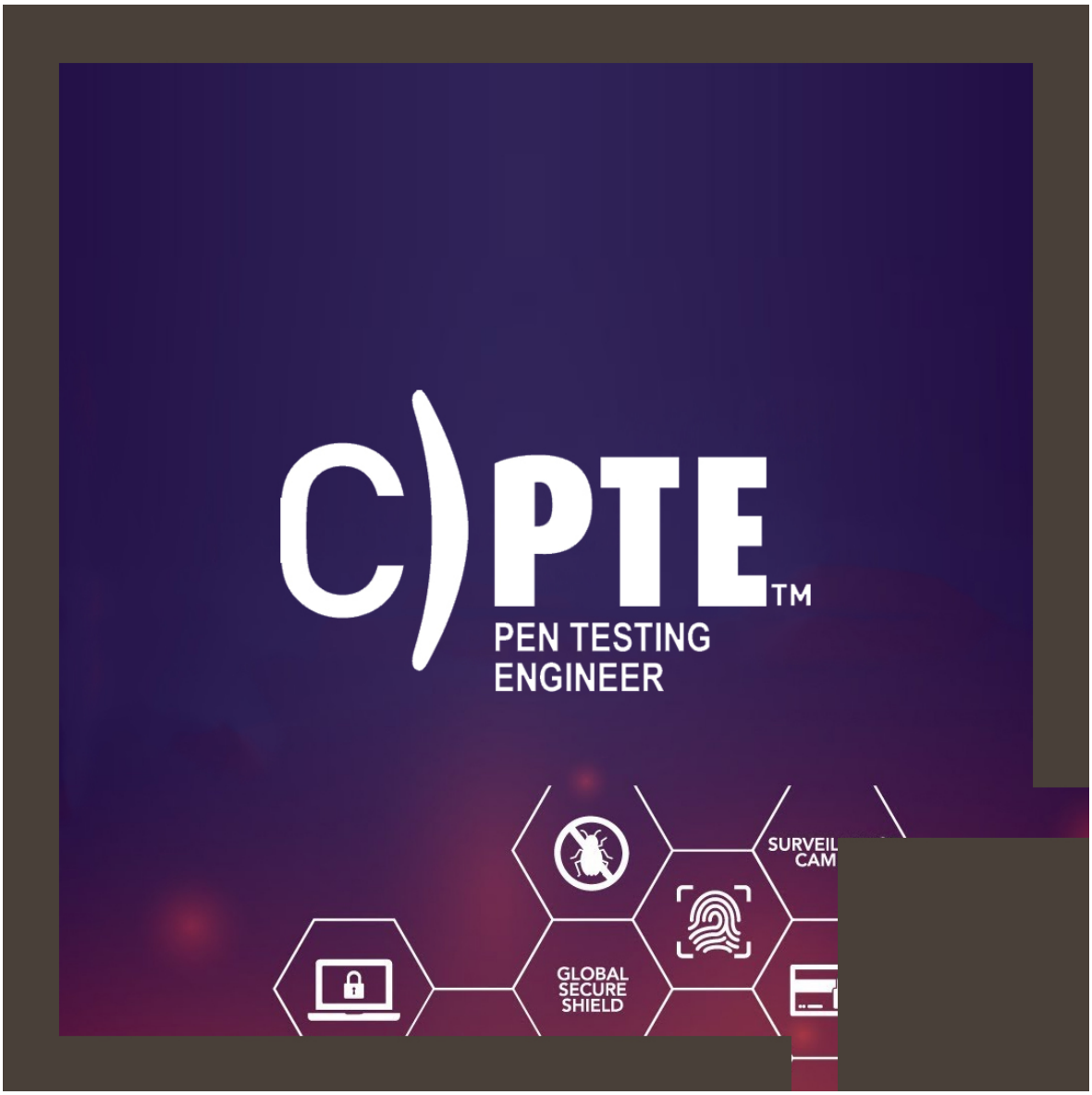
Learning Style: On Demand

Technology:

Difficulty: Intermediate

Course Duration: 7 Hours

Certified Penetration Testing Engineer



About this course:

A penetration test, or pen-test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations or risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as, end-user adherence to security policies. This Official Mile2® cyber security certification training series covers everything you need to know about becoming a Certified Penetration Testing Engineer. Students will learn about logistics of pen testing, Linux fundamentals, information gathering, detecting live systems, enumeration, vulnerability assessments, malware going undercover, Windows hacking, hacking UNIX/Linux, advanced exploitation techniques, pen testing wireless networks, networks, sniffing and IDS, injecting the database, attacking web technologies, and project documentation.

The average salary for Certified Pen Tester is **$71,660** per year.

Course Objective:

After completing this course, students will be able to:

- Establish industry acceptable auditing standards with current best practices and policies

Audience:

This course is intended for:

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

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

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

Credly Badge:

Display your Completion Badge And Get The Recognition You Deserve.

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges