Certified Penetration Testing Engineer

Modality: On Demand

Duration: 7 Hours

About this course:

A pen-test or infiltration test is an endeavor to measure the safety of an IT framework by securely attempt to exploit vulnerabilities. Such vulnerabilities may present in services and application flaws, operating systems, risky end-user behavior or inappropriate configuration. These evaluations are also helpful in confirming the effectiveness of defensive systems, along with end-user adherence to security policies. The Official Mile2® cybersecurity certification learning series encompasses everything that you have to understand about become a Certified Penetration Testing Engineer. Candidate will learn about Linux fundamentals, detecting live systems, vulnerability assessments, Windows hacking, advanced exploitation techniques, networks, injecting the database, project documentation, logistics of pen testing, enumeration, malware going undercover, sniffing and IDS, hacking UNIX/Linux, information gathering, penetration testing wireless networks, and attacking web technologies.

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

Course Objective:

After finishing this course, candidates will learn to:

- Develop industry-recognized auditing standards with existing best policies and practices.

Audience:

This course is designed for:

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

Prerequisites:

- At least 1 year of experience in networking technologies
- Good understanding of TCP/IP
- Understanding of Microsoft packages
- Security+, Microsoft, Network+
- Fundamental Understanding of Linux

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