Certified Penetration Testing Engineer

Description:

A Certified Penetration Testing Engineer imagines all of the ways that a hacker can penetrate a data system. You have to go beyond what you learned as an Ethical Hacker because pen testing explores technical and non-technical ways of breaching security to gain access to a system. Our C)PTE course is built on proven hands-on methods utilized by our international group of vulnerability consultants.

In this course you will learn 5 Key Elements of Pen Testing; Information Gathering, Scanning, Enumeration, Exploitation and Reporting. Plus, discover the latest vulnerabilities and the techniques malicious hackers are using to acquire and destroy data. Additionally, you will learn more about the business skills needed to identify protection opportunities, justify testing activities and optimize security controls appropriate to the business needs in order to reduce business risk.

Annual Salary Potential $84,314 AVG/year

Key Course Information

Live Class Duration: 5 Days
CEUs: 40
Language: English
Class Formats Available:

Instructor Led

Self-Study

Live Virtual Training

Suggested Prerequisites:

- Mile2 C)PEH or equivalent knowledge
- 12 months of Networking Experience
- Sound Knowledge of TCP/IP
- Basic Knowledge of Linux
- Microsoft Security experience

Modules/Lessons

Module 1 - Business & Technical Logistics of Pen Testing
Module 2 -Information Gathering Reconnaissance -Passive (External Only)
Module 3 - Detecting Live Systems
Module 4 - Banner Grabbing and Enumeration
Module 5 - Automated Vulnerability Assessment
Module 6 -Hacking an OS
Module 7 -Advanced Assessment and Exploitation Techniques
Module 8 -Evasion Techniques
Module 9 - Hacking with PowerShell
Module 10 - Networks and Sniffing
Module 11 - Hacking Web Tech
Module 12- Mobile and IoT Hacking
Module 13 - Report Writing Basics

Hands-On Labs

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)
Lab 11 – Advanced Vulnerability and Exploitation Techniques
Lab 12 – Network Sniffing/IDS
Lab 13 – Attacking Databases
Lab 14 – Attacking Web Applications

Certified Penetration Testing Engineer

Upon Completion

Upon completion, the Certified Penetration Testing Engineer, C)PTE, candidate will have solid knowledge of testing and reporting procedures which will prepare them for upper management roles within a cybersecurity system. They will be able to competently take the C)PTE exam.

Who Should Attend

- Pen Testers
- Security Officers
- Ethical Hackers
- Network Auditors
- Vulnerability assessors
- System Owners and Managers
- Cyber Security Engineers

Accreditations

Exam Information

The Certified Penetration Testing Engineer exam is taken online through Mile2's Learning Management System and is accessible on you Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1) Pass the most current version of the exam for your respective existing certification
2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

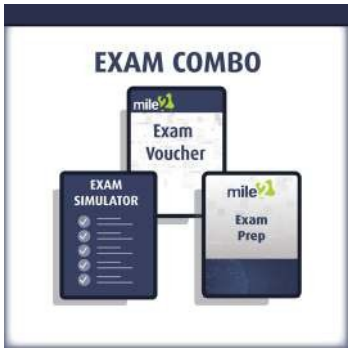
Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options



Detailed Outline:

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

Detailed Lab Outline:

Course Introduction

Lab 1 – Introduction to Pen Testing Setup

a. Section 1 – Recording IPs and Logging into the VMs
b. Section 2 – Research

Lab 2 – Linux Fundamentals

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

Lab 3 – Using tools for reporting

a. Section 1 – Setting up and using magictree

Lab 4 – Information Gathering

b. Section 1 – Google Queries
c. Section 2 – Searching Pastebin
d. Section 3 – Maltego
e. Section 4 – People Search Using the Spokeo Online Tool
f. Section 5 – Recon with Firefox
g. Section 6 – Documentation

Lab 5 – Detecting Live Systems - Scanning Techniques

a. Section 1 – Finding a target using Ping utility
b. Section 2 – Footprinting a Target Using nslookup Tool
c. Section 3 – Scanning a Target Using nmap Tools
d. Section 4 – Scanning a Target Using Zenmap Tools
e. Section 5 – Scanning a Target Using hping3 Utility
f. Section 6 – Make use of the telnet utility to perform banner grabbing
g. Section 7 – Documentation

Lab 6 – Enumeration

a. Section 1 – OS Detection with Zenmap
b. Section 2 – Enumerating a local system with Hyena
c. Section 3 – Enumerating services with nmap

d. Section 4 – DNS Zone Transfer
e. Section 5 – LDAP Enumeration

Lab 7 – Vulnerability Assessments

a. Section 1 – Vulnerability Assessment with SAINT
b. Section 2 – Vulnerability Assessment with OpenVAS

Lab 8 – Software Goes Undercover

a. Section 1 – Creating a Virus

Lab 9 – System Hacking – Windows Hacking

b. Section 1 – System Monitoring and Surveillance
c. Section 2 – Hiding Files using NTFS Streams
d. Section 3 – Find Hidden ADS Files
e. Section 4 – Hiding Files with Stealth Tools
f. Section 5 – Extracting SAM Hashes for Password cracking
g. Section 6 – Creating Rainbow Tables
h. Section 7 – Password Cracking
i. Section 8 – Mimikatz

Lab 10 – System Hacking – Linux/Unix Hacking

a. Section 1 – Taking Advantage of Misconfigured Services
b. Section 2 – Cracking a Linux Password
c. Section 3 – Setting up a Backdoor

Lab 11 – Advanced Vulnerability and Exploitation Techniques

a. Section 1 – Metasploitable Fundamentals
b. Section 2 – Metasploit port and vulnerability scanning
c. Section 3 – Client-side attack with Metasploit
d. Section 4 – Armitage

Lab 12 – Network Sniffing/IDS

a. Section 1 – Sniffing Passwords with Wireshark
b. Section 2 – Performing MitM with Cain
c. Section 3 – Performing MitM with sslstrip

Lab 13 – Attacking Databases

a. Section 1 – Attacking MySQL Database
b. Section 2 – Manual SQL Injection

Lab 14 – Attacking Web Applications

a. Section 1 – Attacking with XSS
b. Section 2 – Attacking with CSRF