Certified Penetration Testing

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

Completion of Mile2 provided training and/or education is not required to achieve any Mile2 certification.

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 01: Business & Technical Logistics of Pen Testing
Module 02: Information Gathering
Module 03: Detecting Live Systems
Module 04 - Banner Grabbing and Enumeration
Module 05: Automated Vulnerability Assessment
Module 06: Hacking an OS
Module 07: Advanced Assessment and Exploitation Techniques
Module 08: Evasion Techniques
Module 09: 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 01: Introduction to Pen Testing Setup
Lab 02: Using Tools for Reporting
Lab 03: Information Gathering
Lab 04: Detecting Live Systems
Lab 05: Enumeration
Lab 06: Vulnerability Assessments
Lab 07: System Hacking (Windows)
Lab 08: Advanced Vulnerability and Exploitation Techniques
Lab 09: AntiVirus Bypass
Lab 10: Cracking Passwords from a Linux System
Lab 11: Hacking with PowerShell
Lab 12: Network Sniffing/IDS
Lab 13: Attacking Web Applications

Certified Penetration Testing

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.

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

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

1) Submit CEUs and Purchase Certification Renewal
   a. Earn and submit 60 CEUs over three years in your Mile2 account.
   b. Purchase Certification Renewal
2) Retake Current Certification Exam

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

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:

Lab 1 – Introduction to Pen Testing Setup

a. Section 1 – Recording IPs and Logging into the VMs
b. Section 2 – Joining the Domain
c. Section 3 – Research

Lab 2 – Using tools for reporting

a. Section 1 – Setup a Shared Folder
b. Section 2 – Setting up and using Dradis CE

Lab 3 – Information Gathering

a. Section 1 – Google Queries
b. Section 2 – Searching Shodan
c. Section 3 – Maltego
d. Section 4 – The many tools of OSINT
e. Section 5 – Recon-ng

Lab 4 – 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

Lab 5 – Enumeration

a. Section 1 – OS Detection with Zenmap
b. Section 2 – Enumerating services with nmap
c. Section 3 – DNS Zone Transfer
d. Section 4 – Enum4linux
e. Section 5 – AD Enumeration

Lab 6 – Vulnerability Assessments

a. Section 1 – Vulnerability Assessment with Rapid7 InsightVM
b. Section 2 – Vulnerability Assessment with OpenVAS

Lab 7 – System Hacking – Windows Hacking

a. Section 1 – Scanning from the Hacked System
b. Section 2 – Using a Keylogger
c. Section 3 – Extracting SAM Hashes for Password cracking
d. Section 4 – Creating Rainbow Tables
e. Section 5 – Password Cracking with Rainbow Tables
f. Section 6 – Password Cracking with Hashcat
g. Section 7 – Mimikatz

Lab 8 – 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 – Using Workspaces in Metasploit
e. Section 5 – Remote Exploitation of Windows Server

Lab 9 – AntiVirus Bypass

a. Section 1 – Bypassing AntiVirus – Not as effective
b. Section 2 – Bypassing AntiVirus Signature Scanning
c. Section 3 – Bypassing Windows Defender

Lab 10 – Cracking Passwords from a Linux System

a. Section 1 – Cracking Linux Passwords
b. Section 2 – Brute-force SSH Accounts

Lab 11 – Hacking with PowerShell

a. Section 1 – Using PowerShell to Crack Passwords
b. Section 2 – Using PowerShell for Enumeration

Lab 12 – Network Sniffing/IDS

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

Lab 13 – Attacking Web Applications

a. Section 1 – OWASP TOP 10 2017 A1: Injection
b. Section 2 – OWASP TOP 10 2017 A2: Broken Authentication
c. Section 3 – OWASP TOP 10 2017 A3: Sensitive Data Exposure
d. Section 4 – OWASP TOP 10 2017 A4: XML External Entities
e. Section 5 – OWASP TOP 10 2017 A5: Broken Access Control
f. Section 6 – OWASP TOP 10 2017 A6: Security Misconfiguration
g. Section 7 – OWASP TOP 10 2017 A7: Cross-Site Scripting
h. Section 8 – OWASP TOP 10 2017 A8: Insecure Deserialization
i. Section 9 – WebApp Scanning