Certified Penetration Testing Consultant

Description:

The Certified Penetration Testing Consultant, C)PTC , course is designed for IT Security Professionals and IT Network Administrators who are interested in taking an in-depth look into specific penetration testing and techniques used against operating systems. This course will teach you the necessary skills to work with a penetration testing team, the exploitation process, and how to create a buffer overflow against programs running on Windows and Linux while subverting features such as DEP and ASLR.

Annual Salary Potential $110,000 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 and C)PTE or equivalent knowledge

- 2 years of experience in Networking Technologies

- Sound Knowledge of TCP/IP

- Computer Hardware Knowledge

Modules/Lessons

Module 1 - Penetration Testing Team Formation
Module 2- NMAP Automation
Module 3 - Exploitation Process
Module 4 - Fuzzing with Spike
Module 5 - Simple Buffer Overflow
Module 6 - Stack Based Windows Buffer Overflow
Module 7 - Web Application Security and Exploitation
Module 8 - Linux Stack Smashing & Scanning
Module 9 - Linux Address Space Layout Randomization
Module 10 - Windows Exploit Protection
Module 11 - Getting Around SEH ASLR
Module 12 - Penetration Testing Report Writing

Hands-On Labs

Lab 1 – Skills Assessment

Lab 2 – Automation Breakdown

Lab 3 – Fuzzing with Spike

Lab 4 – Let's Crash and Callback

Lab 5 – MiniShare for the Win

Lab 6 – Stack Overflow: Did we get root?

Lab 7 – Defeat Me and Lookout ASLR

Lab 8 – Time to Overwrite SHE and ASLR

Upon Completion

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

Who Should Attend

- IS Security Officers
- Cybersecurity Managers/Administrators
- Penetration Testers
- Ethical Hackers
- Auditors

Accreditations

Exam Information

The Certified Penetration Testing Consultant exam consists of two parts:

The first part is a completely hands-on penetration test in which the examinee will find specific flags and write a complete report.

The second part are the exams through the online Mile2's Assessment and Certification System

("MACS"). The examinee will take two exams. One is a few questions selecting the flags found during the hands-on exam and the second is an exam that will take 2 hours and consist of 100 multiple-choice questions.

The hands-on exam requires 4 of 5 systems to be exploited and the 2nd exam requires a 70% passing score. The online exams are accessible in your mile2.com 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:

Course Introduction

Module 1 – Pentesting Team Foundation

a. Project Management
b. Pentesting Metrics
c. Team Roles, Responsibilities and Benefits

Lab Exercise – Skills Assessment

Module 2 – NMAP Automation

a. NMAP Basics
b. NMAP Automation
c. NMAP Report Documentation

Lab Exercise – Automation Breakdown

Module 3 – Exploitation Processes

a. Purpose
b. Countermeasures
c. Evasion
d. Precision Strike
e. Customized Exploitation
f. Tailored Exploits
g. Zero Day Angle
h. Example Avenues of Attack
i. Overall Objective of Exploitation

Module 4 – Fuzzing with Spike

a. Vulnserver
b. Spike Fuzzing Setup
c. Fuzzing a TCP Application
d. Custom Fuzzing Script

Lab Exercise – Fuzzing with Spike

Module 5 – Privilege Escalation

a. Exploit-DB
b. Immunity Debugger
c. Python
d. Shellcode

Lab Exercise – Let's Crash and Callback

\

Module 6 – Stack Based Windows Buffer Overflow

a. Debugger
b. Vulnerability Research
c. Control EIP, Control the Crash
d. JMP ESP Instruction
e. Finding the Offset
f. Code Execution and Shellcode
g. Does the Exploit Work?

Lab Exercise – MiniShare for the Win

Module 7 – Web Application Security and Exploitation

a. Web Applications
b. OWASP Top 10 - 2017
c. Zap
d. Scapy

Module 8 – Linux Stack Smashing

a. Exploiting the Stack on Linux

Lab Exercise – Stack Overflow. Did we get root?

Module 9 – Linux Address Space Layout Randomization

b. Stack Smashing to the Extreme

Lab Exercise – Defeat Me and Lookout ASLR

Module 10 – Windows Exploit Protection

c. Introduction to Windows Exploit Protection
d. Structured Exception Handling
e. Data Execution Prevention (DEP)
f. SafeSEH/SEHOP

Module 11 – Getting Around SEH and ASLR (Windows)

a. Vulnerable Server Setup
b. Time to Test it Out
c. “Vulnserver” meets Immunity
d. VulnServer Demo

Lab Exercise – Time to overwrite SEH and ASLR

Module 12 – Penetration Testing Report Writing