Certified Penetration Testing Consultant

KEY DATA

Course Name: C)PTC V2

Duration: 5 days
Language: English

Class Format:
- Instructor-led
- Live Online Training

Prerequisites:
- C)PTE or equivalent knowledge
- A minimum of 24 months experience in Networking Technologies
- Sound knowledge of TCP/IP
- Computer hardware knowledge

Student Materials:
- Student Workbook
- Student Lab Guide
- Student Prep Guide

Certification Exams:
- Mile2 C)PTC

CPEs: 40 Hours

WHO SHOULD ATTEND?

- IS Security Officers
- Cyber Security Managers/Admins
- Penetration Testers
- Ethical Hackers
- Auditors

COURSE OVERVIEW

The vendor neutral **Certified Penetration Testing Consultant** course is designed for IT Security Professionals and IT Network Administrators who are interested in taking an in-depth look into specific Penetration tests and techniques against operating systems. This course will teach you the necessary skills to work as a penetration testing team, the exploitation process, how to create a buffer overflow against programs running on Window and Linux while subverting features such as DEP and ASLR. This course will guide you through OWASP Top 10, teach you how to create shellcode to gain remote code execution, and understand and build different proof of concept code based on exploits pulled from exploit-db and testing using a debugger. The course starts by explaining how to build the right penetration testing team, covers scanning with NMAP, leading into the exploitation process, a little fuzzing with spike to help guide our proof of concept code, writing buffer overflows, understanding OWASP, Linux stack smashing, Windows exploit protection and getting around those protection methods, a section on report writing, and capping off the course with a scenario that will you're your skills as a penetration testing team.

This course uses in-depth lab exercises after most modules. Students may spend 16 hours+ performing labs that emulate a real-world Pen Testing and exploit development.

Pen Testing Hacking Career

C)VA™ Certified Vulnerability Assessor

C)PEH™ CERTIFIED PROFESSIONAL ETHICAL HACKER

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

C)PTC™ * CERTIFIED PENETRATION TESTING CONSULTANT

All Combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide)
- Exam Prep Questions
- Exam
- Cyber Range Lab

ias™ INFORMATION ASSURANCE SERVICES · pt™ PENETRATION TESTING · dr™ DISASTER RECOVERY · gs™ GENERAL SECURITY · SC™ SECURE CODING · vbp™ VIRTUALIZATION BEST PRACTICES · ws™ WIRELESS SECURITY · cf™ COMPUTER FORENSICS

C)PTC™ CERTIFIED PENETRATION TESTING CONSULTANT

mile2® CYBER SECURITY CERTIFICATIONS

ACCREDITATIONS

COMMITTEE ON NATIONAL SECURITY SYSTEMS — CNSS — SYSTEMS SECURITY FOR THE 21st CENTURY

NICCS™ NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

DEPARTMENT OF JUSTICE — FEDERAL BUREAU OF INVESTIGATION — FIDELITY BRAVERY INTEGRITY

UPON COMPLETION

Upon completion, **Certified Penetration Testing Consultant** students will be able to both establish an industry acceptable pen testing process as well as be prepared to competently take the C)PTC exam.

EXAM INFORMATION

The **Certified Penetration Testing Consultant** exam consists of two parts. Part 1 is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions.

macs Assessment & Certification System

COURSE DETAILS

Module 1: Pen 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
Module 9: Linux Address Space Layout Randomization
Module 10: Windows Exploit Protection
Module 11: Getting Around SEH and ASLR
Module 12: Penetration Testing Report Writing

LABORATORY EXERCISES

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 SEH and ASLR

C)PTC™ CERTIFIED PENETRATION TESTING CONSULTANT

mile2® CYBER SECURITY CERTIFICATIONS

DETAILED MODULE DESCRIPTION

Module 1 – Pentesting Team Formation
Section 1 – Project Management
Section 2 – Pentesting Metrics
Section 3 – Team Roles, Responsibilities and Benefits
Lab Exercise – Skills Assessment

Module 2 – NMAP Automation
Section 1– NMAP Basics
Section 2 – NMAP Automation
Section 3 – NMAP Report Documentation
Lab Exercise – Automation Breakdown

Module 3 – Exploitation Process
Section 1 – Purpose
Section 2 – Countermeasures
Section 3 – Evasion
Section 4 – Precision Strike
Section 5 – Customized Exploitation
Section 6 – Tailored Exploits
Section 7 – Zero Day Angle
Section 8 – Example Avenues of Attack
Section 9 – Overall Objective of Exploitation

Module 4 – Fuzzing with Spike
Section 1 – Vulnserver
Section 2 – Spike Fuzzing Setup
Section 3 – Fuzzing a TCP Application
Section 4 – Custom Fuzzing Script
Lab Exercise – Fuzzing with Spike

Module 5 – Simple Buffer Overflow
Section 1 – Exploit-DB
Section 2 – Immunity Debugger
Section 3 – Python
Section 4 - Shellcode
Lab Exercise – Let's Crash and Callback

Module 6 – Stack Based Windows Buffer Overflow
Section 1 – Debugger
Section 2 – Vulnerability Research
Section 3 – Control EIP, Control the Crash
Section 4 – JMP ESP Instruction
Section 5 – Finding the Offset
Section 6 – Code Execution and Shellcode
Section 7 – Does the Exploit Work?
Lab Exercise – MiniShare for the Win

Module 7 – Web Application Security and Exploitation
Section 1 – Web Applications
Section 2 – OWASP Top 10 - 2017
Section 3 – Zap
Section 4 – Scapy

Module 8 – Linux Stack Smashing
Section 1 – Exploiting the Stack on Linux
Lab Exercise – Stack Overflow. Did we get root?

Module 9 – Linux Address Space Layout Randomization
Section 1 – Stack Smashing to the Extreme
Lab Exercise – Defeat Me and Lookout ASLR

Module 10 – Windows Exploit Protection
Section 1 – Introduction to Windows Exploit Protection
Section 2 - Structured Exception Handling
Section 3 – Data Execution Prevention (DEP)
Section 4 – SafeSEH/SEHOP

Module 11 – Getting Around SEH and ASLR (Windows)

Section 1 – Vulnerable Server Setup
Section 2 – Time to Test it Out
Section 3 - “Vulnserver” meets Immunity
Section 4 – VulnServer Demo
Lab Exercise – Time to overwrite SEH and ASLR

Module 12 – Penetration Testing Report Writing

Section 1 – Reporting