Training: Mile2
C)PTC - Certified Penetration Testing Consultant

TRAINING GOALS:

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.

Upon completion

Upon completion, the Certified Penetration Testing Consultant, C)PTC, 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)PTC exam.

Each participant in an authorized Mile2 C)PTC training held in Compendium CE will receive a free CPTC Certified Penetration Testing Consultant exam voucher.

Who Should Attend

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

Mile2® is:

ACCREDITED by the NSA CNSS 4011-4016 https://mile2.com/accreditations/

MAPPED to NIST / Homeland Security NICCS's Cyber Security Workforce Framework https://mile2.com/niccs/

APPROVED on the FBI Cyber Security Certification Requirement list (Tier 1-3)

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

CONSPECT:

- Pentesting Team Foundation
  - Project Management
  - Pentesting Metrics
  - Team Roles, Responsibilities and Benefits
  - Lab Exercise - Skills Assessment
- NMAP Automation
  - NMAP Basics
  - NMAP Automation
  - NMAP Report Documentation
  - Lab Exercise - Automation Breakdown
- Exploitation Processes
  - Purpose
  - Countermeasures
  - Evasion
  - Precision Strike
  - Customized Exploitation
  - Tailored Exploits
  - Zero Day Angle
  - Example Avenues of Attack
  - Overall Objective of Exploitation
- Fuzzing with Spike
  - Vulnserver
  - Spike Fuzzing Setup
  - Fuzzing a TCP Application
  - Custom Fuzzing Script
  - Lab Exercise - Fuzzing with Spike
- Privilege Escalation
  - Exploit-DB
  - Immunity Debugger
  - Python
  - Shellcode
  - Lab Exercise - Let’s Crash and Callback
- Stack Based Windows Buffer Overflow
  - Debugger

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Vulnerability Research
- Control EIP, Control the Crash
- JMP ESP Instruction
- Finding the Offset
- Code Execution and Shellcode
- Does the Exploit Work?
- Lab Exercise - MiniShare for the Win

- Web Application Security and Exploitation
  - Web Applications
  - OWASP Top 10
  - Zap
  - Scapy
- Module 8 - Linux Stack Smashing
  - Exploiting the Stack on Linux
  - Lab Exercise - Stack Overflow. Did we get root?
- Linux Address Space Layout Randomization
  - Stack Smashing to the Extreme
  - Lab Exercise - Defeat Me and Lookout ASLR
- Windows Exploit Protection
  - Introduction to Windows Exploit Protection
  - Structured Exception Handling
  - Data Execution Prevention (DEP)
  - SafeSEH/SEHOP
- Getting Around SEH and ASLR (Windows)
  - Vulnerable Server Setup
  - Time to Test it Out
  - "Vulnserver" meets Immunity
  - VulnServer Demo
  - Lab Exercise - Time to overwrite SEH and ASLR
- Penetration Testing Report Writing

REQUIREMENTS:

Suggested prerequisites:

- Participation in Mile2’s C)PEH - Certified Professional Ethical Hacker or equivalent knowledge
- Participation in Mile2’s C)PTE - Certified Penetration Testing Engineer or equivalent knowledge

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 2 years of experience in Networking Technologies
- Sound Knowledge of TCP/IP
- Computer Hardware Knowledge

Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Mile2 (course completion).

This course will help prepare you for the Certified Penetration Testing Consultant CPTC exam. 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 hands-on exam requires 4 of 5 systems to be exploited.

The second part are the exams through the online Mile2's Assessment and Certification System ("MACS"). And this exam will take 2 hours and consist of 100 multiplechoice questions, requires a 70% passing score.The online exams are accessible in your mile2.com account.

Each participant in an authorized Mile2 C)PTC training held in Compendium CE will receive a free CPTC Certified Penetration Testing Consultant exam voucher.

TRAINER:

Certified Mile2 Instructor

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007