Training: Mile2
C)PTC - Certified Penetration Testing Consultant

TRANING TERMS

2025-08-05 | 4 days | Kraków / Virtual Classroom
2025-09-02 | 4 days | Warszawa / Virtual Classroom
2025-10-07 | 4 days | Kraków / Virtual Classroom
2025-11-04 | 4 days | Warszawa / Virtual Classroom

TRAINING GOALS:

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 Windows and Linux while subverting features such as DEP and ASLR. This course will guide you through the OWASP Top 10, teach you how to create shellcode to gain remote code execution, as well as, teach you to build and understand 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 test 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.

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.

Who Should Attend:

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

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

Accreditations & Acknowledgements

Mile2® is:

- ACCREDITED by the NSA CNSS 4011-4016
- MAPPED to NIST / Homeland Security NICCS's Cyber Security Workforce Framework
- APPROVED on the FBI Cyber Security Certification Requirement list (Tier 1-3)

CONSPECT:

- Pen Testing Team Formation
  - Project Management
  - Pen testing Metrics
  - Team Roles, Responsibilities and Benefits
  - Lab Exercise – Skills Assessment
- NMAP Automation
  - NMAP Basics
  - NMAP Automation
  - NMAP Report Documentation
  - Lab Exercise –Automation Breakdown
- Exploitation Process
  - 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
- Simple Buffer Overflow
  - Exploit-DB

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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

- Immunity Debugger
- Python
- Shellcode
- Lab Exercise –Let's Crash and Callback

- Stack Based Windows Buffer Overflow
  - Debugger
  - 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 -2017
  - Zap
  - Scapy
- Linux Stack Smashing & Scanning
  - 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 ASLR
  - Vulnerable Server Setup
  - Time to Test it Out
  - Podatny serwer (VulnServer) a odporność
  - VulnServer Demo
  - Lab Exercise –Time to overwrite SEH and ASLR
- Penetration Testing Report Writing

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

- Reporting

REQUIREMENTS:

- C)PTE - Penetration Testing Engineer or equivalent experience.

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 exam, which is available through the on-line 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.

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

TRAINER:

Certified Mile2 Instructor.

ADDITIONAL INFORMATION:

We also recommend further training and certification:

- C)IHE - Certified Incident Handling Engineer
- C)DRE - Certified Disaster Recovery Engineer

Compendium Education Center Ltd.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 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