Training: Mile2
C)PTE - Certified Penetration Testing Engineer

TRAINING GOALS:

The Mile2 Certified Penetration Testing Engineer (CPTE) is an advanced, hands-on penetration testing certification course designed for cybersecurity professionals ready to move beyond foundational ethical hacking and into real-world offensive security work. CPTE develops the mindset, methodology, and technical capability needed to perform authorized security assessments across modern enterprise environments.

The course takes students through the full penetration testing lifecycle, from scoping, rules of engagement, and methodology to reconnaissance, attack surface mapping, controlled exploitation, post-exploitation, credential attacks, lateral movement, evasion concepts, threat simulation, purple team collaboration, and business-focused reporting. Students examine today's complex attack surfaces, including traditional networks, cloud-connected systems, hybrid identity environments, Active Directory, Entra ID, Microsoft 365, web applications, APIs, mobile applications, and enterprise infrastructure.

What makes CPTE advanced is its blend of technical exploitation depth and business-risk communication. Students learn to validate vulnerabilities safely, select payloads based on target context and stability, identify realistic privilege escalation and persistence paths, analyze identity-based attack chains, document evidence clearly, and translate technical findings into meaningful remediation priorities for both technical teams and executive leadership.

CPTE also introduces modern adversary simulation concepts using frameworks such as MITRE ATT&CK, the Cyber Kill Chain, and the Diamond Model, helping students connect offensive testing to detection engineering, incident response, telemetry validation, and continuous security improvement.

For learners pursuing a serious path into professional penetration testing, CPTE provides a practical, structured, and forward-looking roadmap. It is an ideal next step for those preparing for roles such as penetration tester, security engineer, red team operator, offensive security analyst, or security consultant.

Compendium Centrum Edukacyjne Spółka z o.o.
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

Upon completion

- Upon completion, CPTE candidates will be prepared to conduct authorized penetration testing engagements using a structured methodology while translating technical findings into real-world risk, remediation priorities, and executive decision-making.

Each participant in an authorized Mile2 C)PTE training held in Compendium CE will receive a free CPTE Certified Penetration Testing Engineer exam voucher.

Who Should Attend

- CPEH, CVA, CSP
- Pen Testers
- Security Engineers
- Ethical Hackers
- Network Auditors
- Vulnerability assessors
- System Owners
- Cyber Security Engineers
- technical security staff moving into more advanced testing roles.

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)

CONSPECT:

- Module 01: Penetration Testing Methodologies
  - Pen Test Phases
  - Scoping and Legal Boundaries
  - OWASP Testing Framework
- Module 02: Advanced Recon & Attack Surface Mapping
  - Recon Philosophy & Objectives

Compendium Centrum Edukacyjne Spółka z o.o.
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

- DNS, Subdomains, and Certificates
- OSINT & Metadata Intelligence
- Tech Stack & Service Fingerprinting
- Mapping the Attack Surface

- Module 03: Exploitation Techniques (Local & Remote)
  - Understanding Exploitation Process
  - Modern Exploitation Techniques and Shell Management
  - Payload Execution & Stability
- Module 04: Post-Exploitation & Lateral Movement
  - Credential Harvesting & Token Abuse
  - Scanning, Pivoting & Routing Through Compromised Hosts
  - Lateral Movement Techniques
  - Persistence Mechanisms
  - Hiding Persistence and Cleanup
- Module 05: Cloud & Active Directory Exploitation
  - Enterprise Identity and AD Basics for Attackers
  - Local Priv Esc → Domain Admin Escalation Paths
  - Azure/M365 Exploitation - Initial Access to Persistence
  - Hybrid Identity Exploitation Paths (AD Connect, Entra Sync)
  - Real-World Kill Chain Examples (Hybrid Pathways)
- Module 06: Evasion & Payload Crafting
  - EDR & AV Evasion Fundamentals
  - Crafting Payloads with Caution
  - Obfuscation and Execution Techniques
  - Frameworks & Modern C2 Delivery
  - Red Team Tradecraft for Evasion Success
- Module 07: Web, API & Mobile Attacks
  - OWASP Top 10 Deep Dive
  - Advanced API Testing
  - Mobile App Exploitation (Android/iOS)
  - Web Shells and Post-Exploitation via Web
  - Defense Evasion in Web Contexts
- Module 08: Threat Simulation & Attack Chains
  - Threat Simulation Fundamentals
  - Planning and Scoping an Attack Chain
  - Chaining Techniques - From Access to Impact

Compendium Centrum Edukacyjne Spółka z o.o.
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

- Threat Simulation Tools and Frameworks
- Communication, Debriefing, and Lessons Learned

- Module 09: Purple Team Collaboration
  - Introduction to Purple Teaming
  - Building a Purple Team Program
  - Adversary Emulation in Purple Teams
  - Detection Engineering and Alert Tuning
  - Purple Team Exercises - Real World to Lab
  - Continuous Improvement and Lessons Learned
- Module 10: Reporting & Business Risk Analysis
  - Reporting for Technical and Executive Audiences
  - Prioritizing Findings Based on Business Risk
  - Communicating Attack Paths and Exposure Chains
  - Mapping Findings to Frameworks and Controls
  - Strategic Debriefing and Executive Communication
  - Improving the Reporting Lifecycle
- Lab 00: Introduction to Pen Testing Setup
  - Recording IPs and Logging into the VMs
  - Connect Windows VMs to AD
- Lab 01: Pre-Engagement Planning
  - Engaging the Client: Defining the Engagement
  - The Results: Scope, Constraints, and Professional Judgment
  - Setting Up Dradis: Formalizing the Engagement
- Lab 02: External Reconnaissance & Attack Surface Mapping
  - Understanding External Visibility (Passive Recon)
  - Identify Exposed Services and Technologies
  - Active Recon and Surface Mapping
  - Correlation and Attack Path Visualization
  - Reporting & Professional Documentation
- Lab 03: Exploitation Techniques
  - Authenticated Access & Job Abuse
  - Post-Exploitation Evidence Collection
  - Privilege Escalation via Docker Abuse
  - Credential Harvesting & Internal Recon
  - Persistence
  - Reporting in Dradis CE

Compendium Centrum Edukacyjne Spółka z o.o.
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

- Lab 04: Lateral Movement
  - Lateral Movement via Jenkins Agents
  - Recon the Internal Network
  - Pivoting Through DB Connection
- Lab 05: Active Directory Recon and Attacks
  - BloodHound & SharpHound
  - Vertical Privilege Escalation
  - DCSync
- Lab 06: C2 and Evasion
  - Create an Evasive Payload
- Lab 07: Web and API Attacks
  - Getting WebGoat up and Running
  - Application Reconnaissance & Attack Surface Mapping
  - Authorization Testing: Object Access & IDOR
  - API Authorization Failures
  - Session & Identity Trust Abuse
  - Token-Based Authentication Failures
  - Client-Side Controls as an Attack Enabler
- Lab 08: Purple Team Collaboration
  - Detection Engineering Baseline
  - Controlled Adversary Simulation
  - Detection Validation & Gap Analysis
  - Mitigation & Hardening Discussion
  - Bypass Techniques
  - Incident Response & Timeline Reconstruction
- Lab 09: Final Report Assembly & Professional Review
  - Report Quality Audit
  - Strengthening Remediation Guidance
  - Executive Summary Creation
  - Exporting the Final Report
  - Final Professional Review Checklist

REQUIREMENTS:

Suggested prerequisites:

- Mile2 C)PEH or equivalent knowledge

Compendium Centrum Edukacyjne Spółka z o.o.
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

- 12 months of Networking Experience
- Sound Knowledge of TCP/IP
- Basic Knowledge of Linux
- Microsoft Security 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 Engineer CPTE exam, which is available through the on-line Mile2's Learning Management System, and is accessible on your 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.

Each participant in an authorized Mile2 C)PTE training held in Compendium CE will receive a free CPTE Certified Penetration Testing Engineer exam voucher.

TRAINER:

Certified Mile2 Instructor

ADDITIONAL INFORMATION:

Course Student Kit includes:

- Digital Workbook & Study Guide – training materials in the digital form (1-year access)
- Live Cyber Range Labs – cloud-based lab environment (2-week access)
- Exam Prep Guide + Practice Questions – additional materials to help you prepare for the exam
- Official Certification Exam (2 Attempts Included) – exam voucher, with a second free attempt if needed

Compendium Centrum Edukacyjne Spółka z o.o.
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