Szkolenie: Mile2
C)PTE - Certified Penetration Testing Engineer

DOSTĘPNE TERMINY

2026-11-30 | 5 dni | Warszawa / Wirtualna sala *(Termin gwarantowany)*

Cel szkolenia:

Mile2 Certified Penetration Testing Engineer (CPTE) to zaawansowane, praktyczne szkolenie z zakresu testów penetracyjnych, przeznaczone dla specjalistów ds. cyberbezpieczeństwa gotowych wyjść poza podstawy etycznego hakowania (*ethical hacking*) i zmierzyć się z realnymi zadaniami z obszaru bezpieczeństwa ofensywnego (*offensive security*). CPTE rozwija sposób myślenia, metodykę oraz kompetencje techniczne niezbędne do prowadzenia autoryzowanych audytów bezpieczeństwa w nowoczesnych środowiskach korporacyjnych.

Szkolenie przeprowadza uczestników przez pełny cykl życia testów penetracyjnych: od określenia zakresu, zasad współpracy i metodyki, przez rekonesans, mapowanie powierzchni ataku (*attack surface*), kontrolowaną eksploatację (*exploitation*), działania po przejęciu systemu (*post-exploitation*), ataki na poświadczenia, ruch poprzeczny (*lateral movement*), techniki omijania zabezpieczeń (*evasion*), symulację zagrożeń oraz współpracę w modelu *Purple Team*, aż po raportowanie zorientowane na cele biznesowe. Uczestnicy analizują złożone, współczesne powierzchnie ataku, obejmujące tradycyjne sieci, środowiska chmurowe i hybrydowe, tożsamości Active Directory oraz Entra ID (Microsoft 365), a także aplikacje webowe, interfejsy API, aplikacje mobilne i infrastrukturę enterprise.

Zaawansowany charakter CPTE wynika z połączenia pogłębionej pracy technicznej z umiejętnością precyzyjnego komunikowania ryzyka biznesowego. Uczestnicy uczą się bezpiecznie walidować podatności, dobierać ładunki (*payloads*) do kontekstu i stabilności celu, identyfikować realistyczne ścieżki podnoszenia uprawnień (*privilege escalation*) i utrzymania dostępu (*persistence*), a także analizować łańcuchy ataków oparte na tożsamości. Przyswajają również umiejętność jasnego dokumentowania dowodów oraz przekładania ustaleń technicznych na priorytety naprawcze (*remediation*) zrozumiałe zarówno dla zespołów inżynieryjnych, jak i kadry zarządzającej.

CPTE wprowadza ponadto nowoczesne koncepcje symulacji działań przeciwnika (*adversary simulation*) z wykorzystaniem uznanych standardów, takich jak MITRE ATT&CK, Cyber Kill Chain oraz Diamond Model. Pomaga to powiązać testowanie ofensywne z inżynierią detekcji (*detection engineering*), reagowaniem na incydenty, walidacją telemetrii oraz ciągłym doskonaleniem poziomu

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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

bezpieczeństwa organizacji.

Dla osób budujących profesjonalną ścieżkę kariery w obszarze testów penetracyjnych, certyfikacja CPTE stanowi praktyczny, uporządkowany i kompleksowy przewodnik rozwoju. To idealny krok dla specjalistów przygotowujących się do ról takich jak *penetration tester*, *security engineer*, *red team operator*, *offensive security analyst* czy *security consultant*.

Po ukończeniu szkolenia

- Po ukończeniu szkolenia uczestnicy będą przygotowani do prowadzenia profesjonalnych testów penetracyjnych z wykorzystaniem ustrukturyzowanej metodyki, a także do przekładania wykrytych podatności technicznych na realne ryzyko biznesowe, priorytety naprawcze oraz decyzje zarządcze. Zdobędą również wiedzę niezbędną do przystąpienia do egzaminu certyfikacyjnego CPTE.

Każdy uczestnik autoryzowanego szkolenia Mile2 C)PTE realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin CPTE Certified Penetration Testing Engineer.

Dla kogo przeznaczone jest szkolenie:

- CPEH, CVA, CSP
- Pen Testers
- Security Engineers
- Ethical Hackers
- Network Auditors
- Vulnerability assessors
- System Owners
- Cyber Security Engineers
- techniczni specjaliści ds. bezpieczeństwa przechodzący do bardziej zaawansowanych ról zawodowych

Mile2® jest:

- ACCREDITED przez NSA CNSS 4011-4016 https://mile2.com/accreditations/
- MAPPED do NIST / Homeland Security NICCS Cyber Security Workforce Framework https://mile2.com/niccs/

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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- APPROVED na liście FBI Cyber Security Certification Requirement list (Tier 1-3)

Plan szkolenia:

- Moduł 01: Metodyki testów penetracyjnych
  - Fazy testów penetracyjnych (Pen Test Phases)
  - Określanie zakresu i granic prawnych (Scoping & Legal Boundaries)
  - Ramowe zasady testowania OWASP (OWASP Testing Framework)
- Moduł 02: Zaawansowany rekonesans i mapowanie powierzchni ataku
  - Filozofia i cele rekonesansu (Recon)
  - Rekordy DNS, poddomeny i certyfikaty
  - OSINT i pozyskiwanie danych z metadanych (Metadata Intelligence)
  - Identyfikacja stosu technologicznego i usług (Tech Stack & Service Fingerprinting)
  - Mapowanie powierzchni ataku (Attack Surface Mapping)
- Moduł 03: Techniki eksploatacji - lokalne i zdalne
  - Zrozumienie procesu eksploatacji
  - Nowoczesne techniki eksploatacji i zarządzanie powłokami (Shell Management)
  - Wykonywanie ładunków (Payload Execution) i stabilność połączenia
- Moduł 04: Post-eksploatacja i ruch poprzeczny (Post-Exploitation & Lateral Movement)
  - Pozyskiwanie poświadczeń (Credential Harvesting) i nadużywanie tokenów (Token Abuse)
  - Skanowanie, tunelowanie (Pivoting) i trasowanie przez przejęte hosty
  - Techniki ruchu poprzecznego (Lateral Movement)
  - Mechanizmy utrzymania dostępu (Persistence)
  - Ukrywanie obecności i czyszczenie śladów (Cleanup)
- Moduł 05: Eksploatacja środowisk chmurowych i Active Directory
  - Tożsamość w przedsiębiorstwie i podstawy AD z perspektywy atakującego
  - Ścieżki eskalacji uprawnień: od lokalnego użytkownika do Domain Admina
  - Eksploatacja Azure / M365 - od uzyskania dostępu (Initial Access) do utrzymania obecności
  - Ścieżki eksploatacji tożsamości hybrydowej (AD Connect, Entra Sync)
  - Praktyczne przykłady łańcuchów ataku (Kill Chain) w środowiskach hybrydowych
- Moduł 06: Omijanie zabezpieczeń i tworzenie ładunków (Evasion & Payload Crafting)
  - Podstawy omijania systemów EDR i AV (EDR & AV Evasion)
  - Bezpieczne i kontrolowane tworzenie ładunków (Payloads)
  - Techniki zaciemniania kodu (Obfuscation) i egzekucji
  - Frameworki i nowoczesne metody dostarczania C2
  - Praktyki i warsztat Red Teamu w kontekście skutecznej ewazji

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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Moduł 07: Ataki na aplikacje webowe, API i urządzenia mobilne
  - Szczegółowa analiza OWASP Top 10
  - Zaawansowane testy bezpieczeństwa API
  - Eksploatacja aplikacji mobilnych (Android / iOS)
  - Web Shelle i post-eksploatacja z poziomu aplikacji webowych
  - Omijanie mechanizmów obronnych w kontekście aplikacji webowych
- Moduł 08: Symulacja zagrożeń i łańcuchy ataków (Threat Simulation & Attack Chains)
  - Podstawy symulacji zagrożeń (Threat Simulation)
  - Planowanie i określanie zakresu łańcucha ataku (Attack Chain)
  - Łączenie technik ataków - od uzyskania dostępu do wywarcia wpływu (Impact)
  - Narzędzia i frameworki do symulacji zagrożeń
  - Komunikacja, podsumowanie (Debriefing) i wnioski powdrożeniowe (Lessons Learned)
- Moduł 09: Współpraca w modelu Purple Team (Purple Team Collaboration)
  - Wprowadzenie do metodyki Purple Teaming
  - Budowanie programu Purple Team w organizacji
  - Emulacja przeciwnika (Adversary Emulation) w ćwiczeniach Purple Team
  - Inżynieria detekcji (Detection Engineering) i dostrajanie alertów
  - Ćwiczenia Purple Team - od scenariuszy rzeczywistych do środowiska laboratoryjnego
  - Ciągłe doskonalenie i wnioski z ćwiczeń
- Moduł 10: Raportowanie i analiza ryzyka biznesowego
  - Tworzenie raportów dla odbiorców technicznych oraz kadry zarządzającej (Executive)
  - Priorytetyzacja podatności na podstawie ryzyka biznesowego
  - Komunikacja ścieżek ataku i łańcuchów podatności
  - Mapowanie wykrytych podatności na standardy, normy i mechanizmy kontrolne
  - Podsumowanie strategiczne i komunikacja z zarządem
  - Usprawnianie cyklu życia raportu (Reporting Lifecycle)
- Lab 00: Konfiguracja środowiska testowego
  - Rejestracja adresów IP i logowanie do maszyn wirtualnych (VM)
  - Dołączanie maszyn wirtualnych Windows do domeny AD
- Lab 01: Planowanie etapu Pre-Engagement
  - Interakcja z klientem: definiowanie zakresu projektu
  - Wyniki analizy: zakres, ograniczenia i ocena ekspercka
  - Konfiguracja narzędzia Dradis: formalizacja projektu
- Lab 02: Zwiad zewnętrzny i mapowanie powierzchni ataku
  - Analiza widoczności zewnętrznej (zwiad pasywny / Passive Recon)
  - Identyfikacja wystawionych usług i technologii

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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Zwiad aktywny (Active Recon) i mapowanie powierzchni ataku
- Korelacja danych i wizualizacja ścieżek ataku
- Raportowanie i profesjonalna dokumentacja

- Lab 03: Techniki eksploatacji
  - Uwierzytelniony dostęp i nadużywanie zadań harmonogramu (Job Abuse)
  - Zbieranie dowodów na etapie post-eksploatacji
  - Eskalacja uprawnień poprzez nadużycie usługi Docker
  - Pozyskiwanie poświadczeń (Credential Harvesting) i zwiad wewnętrzny
  - Utrzymanie dostępu (Persistence)
  - Raportowanie w Dradis CE
- Lab 04: Ruch poprzeczny (Lateral Movement)
  - Ruch poprzeczny z wykorzystaniem agentów Jenkins
  - Zwiad sieci wewnętrznej
  - Tunelowanie ruchu (Pivoting) poprzez połączenia z bazą danych
- Lab 05: Zwiad i ataki na Active Directory
  - Wykorzystanie narzędzi BloodHound i SharpHound
  - Pionowa eskalacja uprawnień (Vertical Privilege Escalation)
  - Przeprowadzenie ataku DCSync
- Lab 06: Środowiska C2 i ewazja
  - Tworzenie ładunku omijającego zabezpieczenia (Evasive Payload)
- Lab 07: Ataki na Web i API
  - Uruchomienie i konfiguracja środowiska WebGoat
  - Zwiad aplikacji i mapowanie powierzchni ataku
  - Testowanie autoryzacji: dostęp do obiektów i podatności IDOR
  - Błędy w autoryzacji API
  - Nadużycia sesji i relacji zaufania tożsamości
  - Błędy w mechanizmach uwierzytelniania opartych na tokenach
  - Mechanizmy po stronie klienta (Client-Side Controls) jako wektor ataku
- Lab 08: Współpraca Purple Team
  - Tworzenie punktu odniesienia dla inżynierii detekcji (Detection Engineering Baseline)
  - Kontrolowana symulacja przeciwnika
  - Weryfikacja detekcji i analiza luk w zabezpieczeniach (Gap Analysis)
  - Dyskusja nad łagodzeniem zagrożeń (Mitigation) i utwardzaniem konfiguracji (Hardening)
  - Techniki omijania zabezpieczeń (Bypass Techniques)
  - Reagowanie na incydenty i rekonstrukcja osi czasu (Timeline Reconstruction)
- Lab 09: Przygotowanie raportu końcowego i przegląd profesjonalny

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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Audyt jakości raportu
- Wzmocnienie i uszczegółowienie zaleceń naprawczych (Remediation Guidance)
- Tworzenie podsumowania dla kierownictwa (Executive Summary)
- Eksport raportu końcowego
- Lista kontrolna ostatecznego przeglądu profesjonalnego (Final Review Checklist)

Wymagania:

Sugerowane wymagania wstępne:

- Mile2 C)PEH lub równoważna wiedza
- 12 miesięcy doświadczenia w obszarze sieci
- Dobra znajomość TCP/IP
- Podstawowa znajomość Linux
- Doświadczenie z Microsoft Security

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia wystawiony imiennie oraz na firmę sygnowany przez firmę Mile2.

Ponadto kurs ten przygotowuje uczestników do certyfikowanego egzaminu Certified Penetration Testing Engineer CPTE, który jest realizowany za pośrednictwem systemu egzaminacyjnego Mile2's Learning Management System, z poziomu konta mile2.com. Egzamin trwa około 2 godzin i składa się ze 100 pytań wielokrotnego wyboru. Aby uzyskać certyfikację, wymagany jest wynik co najmniej 70%.

Każdy uczestnik autoryzowanego szkolenia Mile2 C)PTE realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin CPTE Certified Penetration Testing Engineer.

Prowadzący:

Autoryzowany instruktor Mile2 (Certified Mile2 Instructor).

Informacje dodatkowe:

Pakiet uczestnika szkolenia (Course Student Kit) obejmuje:

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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Digital Workbook & Study Guide – materiały szkoleniowe w wersji elektronicznej (roczny dostęp)
- Live Cyber Range Labs – środowisko laboratoryjne dostępne w chmurze (2 tygodniowy dostęp)
- Exam Prep Guide + Practice Questions – dodatowe materiały przygotowujące do egzaminu
- Official Certification Exam (2 Attempts Included) – voucher egzaminacyjny wraz drugi darmowym podejściem jeżeli byłoby potrzebne

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.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001