Szkolenie: Mile2
C)PEH - Certified Professional Ethical Hacker

DOSTĘPNE TERMINY

2026-11-23 | 5 dni | Virtual Classroom

Cel szkolenia:

Aby skutecznie chronić system informatyczny, trzeba umieć spojrzeć na niego oczami atakującego. Szkolenie certyfikacyjne Certified Professional Ethical Hacker stanowi podstawę ścieżki kursów Mile2 z zakresu testów penetracyjnych, ponieważ uczy myślenia jak hacker.

Najpierw poznasz wartość oceny podatności (vulnerability assessment). Następnie dowiesz się, jak wykorzystywać wyniki takich ocen do wprowadzania realnych i skutecznych zmian w bezpieczeństwie systemu informatycznego. Dodatkowo omówimy, jak działają malware oraz destrukcyjne wirusy, a także jak wdrażać działania reakcyjne i prewencyjne w kontekście włamań do sieci.

Po ukończeniu

- Po ukończeniu szkolenia uczestnik będzie przygotowany do przystąpienia do egzaminu C)PEH.

Każdy uczestnik autoryzowanego szkolenia Mile2 C)PEH realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin CPEH Certified Professional Ethical Hacker.

Dla kogo

- Właściciele zasobów informacyjnych (IS Security Owners)
- Security Officers
- Ethical Hackers
- Właściciele informacji (Information Owners)
- Testerzy penetracyjni (Penetration Testers)
- Właściciele systemów i menedżerowie (System Owners and Managers)
- Inżynierowie cyberbezpieczeństwa (Cyber Security Engineers)

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

Mile2® jest:

- ACCREDITED przez NSA CNSS 4011-4016 https://mile2.com/accreditations/
- MAPPED do NIST / Homeland Security NICCS's Cyber Security Workforce Framework https://mile2.com/niccs/
- APPROVED na liście wymagań certyfikacyjnych FBI Cyber Security Certification Requirement (Tier 1-3)

Plan szkolenia:

- Moduł 1 - Wprowadzenie do Ethical Hacking
  - Czym jest Ethical Hacking?
  - Threat Actors i motywacje
  - Sposób myślenia hackera i metodyki działania
  - Zasady współpracy (Rules of Engagement) i profesjonalne standardy postępowania
  - Dylematy etyczne i „szare strefy”
  - Rozwoju zawodowy
- Moduł 2 - Podstawy cyberbezpieczeństwa
  - Kluczowe zasady cyberbezpieczeństwa
  - Podstawy architektury bezpieczeństwa
  - Niezbędne mechanizmy kontroli bezpieczeństwa (security controls)
  - Ład bezpieczeństwa (security governance) i polityki
  - Zastosowanie kontroli i architektury w testach
  - Ryzyko, zgodność (compliance) i punkty kontrolne
- Moduł 3 - Rekonesans i enumeracja
  - Pasywny vs Aktywny rekonesans
  - Praktyczne narzędzia stosowane w rekonesansie
  - Techniki enumeracyjne
  - Rekonesans w praktyce: Nmap, skrypty i enumeracja
  - Scenariusze ćwiczeniowe i raportowanie
  - Projekt końcowy i podsumowanie
- Moduł 4 - Kryptografia
  - Podstawy kryptografii
  - Kryptografia symetryczna
  - Kryptografia asymetryczna
  - Funkcja skrótu (hashing)

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

- Hybrydowe systemy crypto
- Quantum Cryptography
- Nowe kierunki i rozwój kryptografii
- Atakowanie słabej kryptografii: wartości skrótu, klucze i rzeczywiste przykłady błędów

- Moduł 5 - Skanowanie w poszukiwaniu podatności oraz ich analiza
  - Zrozumienie Vulnerability Assessment
  - Metodyki Vulnerability Assessment
  - Interpretacja i walidacja podatności
  - Priorytetyzacja ryzyk w VA
  - Czym jest Patch Management?
  - Różne typy patchy
- Moduł 6 - Ataki na aplikacje i serwisy internetowe
  - Wyjaśnienie OWASP Top 10
  - Łączenie OWASP i CWE w pracy testerów penetracyjnych
  - API Top 10
- Moduł 7 - Eksploatacja i post-eksploatacja
  - Podstawy eksploatacja
  - Exploit Frameworks w praktyce
  - Podstawy post-eksploatacja
  - Pivoting i Lateral Movement
  - Podstawy eksploatacji chmury
- Moduł 8 - Inżynieria społeczna
  - Koncepcje i psychologia inżynierii społecznej
  - Phishing i cyfrowe oszustwa (digital deception)
  - Pretexting i taktyki osobiste (in-person)
  - Ataki z wykorzystaniem porzuconych nośników USB (USB drops) i ataki na urządzenia
  - Narzędzia inżynierii społecznej i ładunki złośliwe (payloady)
  - Studia przypadków (case studies) i działania w terenie
- Moduł 9 - Testy penetracyjne sieci bezprzewodowych
  - Rekonesans (Recon) i enumeracja sieci Wi-Fi
  - Narzędzia Wi-Fi
  - Sniffing (Podsłuch sieciowy)
  - Ataki na uwierzytelnianie (Authentication Attacks)
  - Rogue AP (Nieautoryzowane punkty dostępu)
  - Eksploity Wi-Fi (Wi-Fi Exploits)
  - Ocena zagrożeń (Threat Assessment)

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 10 - Raportowanie i etyka
  - Rola raportowania w Ethical Hacking
  - Pisanie skutecznych raportów
  - Etyka w Ethical Hacking
  - Rozwój zawodowy i odpowiedzialność
- Lab 0 - Przygotowanie środowiska
  - Zapisywanie adresów IP i logowania do VM
  - Analiza
- Lab 1 - Identyfikacja person hackera
  - Studia przypadków (Case Studies)
- Lab 2 - Analiza i profilowanie sprawców ataków (Threat Actors)
  - Dochodzenie (Investigation)
- Lab 3 - Przygotowanie propozycji testów penetracyjnych (Pentest Proposal)
  - Symulacja zlecenia (Simulated Engagement Roleplay)
- Lab 4 - Mapowanie CIA i AAA do rzeczywistych incydentów
  - Incydent 01 - Tesla Data Leak via Insider Threat
  - Incydent 02 - Pegasus Airlines AWS Misconfiguration
  - Incydent 03 - Schneider Electric Ransomware Attack
- Lab 5 - Eksploracja modeli kontroli dostępu w Windows
  - Konfiguracja użytkowników, grup i folderów
  - Zastosowanie DAC (Discretionary Access Control)
  - Zastosowanie RBAC (Role-Based Access Control)
  - Testowanie dostępu lokalnie
- Lab 6 - Klasyfikacja mechanizmów kontroli bezpieczeństwa (Security Controls)
- Lab 7 - Dopasowanie do cyklu życia ataku hackerskiego + narzędzia do rekonesansu
- Lab 8 - Pasywny vs Aktywny rekonesans
  - Pasywny rekonesans
  - Aktywny rekonesns
- Lab 9 - WHOIS, Google Dorking, Shodan
  - Whois lookup
  - Google Dorking
  - Shodan
  - Wykorzystanie wcześniej udokumentowanych danych
- Lab 10 - Enumeracja DNS i SMB
  - Enumeracja DNS
  - Enumeracja SMB

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

- Lab 11 - Nmap i podstawy skryptowania
  - Podstawowe skanowanie Nmap
  - Nmap Scripting Engine (NSE)
  - Skryptowanie w Bash
- Lab 12 - Kryptografia
  - Generowanie funkcji skrótu
  - Podstawy algorytmów kryptograficznych
  - Korzystanie z narzędzia BitLocker
  - Bezpieczne usuwanie plików (niszczenie danych/shredding)
- Lab 13 - Zarządzanie ryzykiem i ocena podatności (Vulnerability Assessment)
  - Wyszukiwanie informacji o podatnościach CVE w internecie
  - Przeprowadzanie wewnętrznej oceny podatności (Vulnerability Assessment)
  - Przeprowadzanie oceny podatności (Vulnerability Assessment) online
  - Skanowanie podatności z wykorzystaniem serwera Nessus Essentials
- Lab 14 - OWASP Top 10
  - Setup
  - A01: Broken Access Control
  - A02: Cryptographic Failures
  - A03: Injection
  - A05: Security Misconfiguration
  - A06: Vulnerable Components
  - A07: Authentication Failures
  - A09: Logging Failures
  - A10: Server-Side Request Forgery
- Lab 15 - Zaawansowane techniki badania podatności i eksploitacji
  - Podstawy laboratorium Metasploitable
  - Skanowanie portów i podatności z użyciem frameworka Metasploit
  - Ataki po stronie klienta (client-side) z wykorzystaniem Metasploit
  - Zarządzanie projektami przy użyciu obszarów roboczych (Workspaces) w Metasploit
- Lab 16 - Bezpieczeństwo sieci bezprzewodowych (Wireless Security) - opcjonalnie
  - Łamanie zabezpieczeń WPA2 z wykorzystaniem AirCrack-ng
  - Łamanie zabezpieczeń WPA2 z wykorzystaniem Wifite

Wymagania:

Sugerowane wymagania wstępne:

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

- Udział w szkoleniu Mile2’s C)SP - Certified Security Principles
- 12 miesięcy doświadczenia w IT
- 12 miesięcy doświadczenia w obszarze sieci

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 Professional Ethical Hacker CPEH, 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)PEH realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin CPEH Certified Professional Ethical Hacker.

Prowadzący:

Autoryzowany instruktor Mile2 (Certified Mile2 Instructor).

Informacje dodatkowe:

Pakiet uczestnika szkolenia (Course Student Kit) obejmuje:

- 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