Training: Mile2
C)PEH - Certified Professional Ethical Hacker

TRANING TERMS

2026-11-23 | 5 days | Virtual Classroom

TRAINING GOALS:

To protect an information system, you need to be able to see that system through the eyes of the attacker. The Certified Professional Ethical Hacker certification course is the foundational training to Mile2's line of penetration testing courses because it teaches you to think like a hacker.

First, you will learn the value of vulnerability assessments. Then, you will discover how to use those assessments to make powerful changes in an information system's security. Additionally, you will learn how malware and destructive viruses' function and how to implement counter response and preventative measures when it comes to a network hack.

Upon completion

- Upon completion, the Certified Professional Ethical Hacker candidate will be able to competently take the C)PEH exam.

Each participant in an authorized Mile2 C)PEH training held in Compendium CE will receive a free CPEH Certified Professional Ethical Hacker exam voucher.

Who Should Attend

- IS Security Owners
- Security Officers
- Ethical Hackers
- Information Owners
- Penetration Testers
- System Owners and Managers

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

- Cyber Security Engineers

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 1 - Introduction to Ethical Hacking
  - What is Ethical Hacking?
  - Threat Actors and Motivations
  - Hacker mindsets and methodologies
  - Rules of Engagement and Professional Conduct
  - Ethical Dilemmas and Gray Areas
  - Career Foundations
- Module 2 - Cybersecurity Foundation
  - Core Cybersecurity Principles
  - Security Architecture Fundamentals
  - Essential Security Controls
  - Security Governance and Policy
  - Applying Controls and Architecture in Testing
  - Risk, Compliance, and Controls
- Module 3 - Reconnaissance & Enumeration
  - Passive vs Active Reconnaissance
  - Practical Recon Tools
  - Enumeration Techniques
  - Applied Recon: Nmap, Scripting, and Enumeration
  - Practice Scenarios and Reporting
  - Capstone & Reflection
- Module 4 - Cryptography
  - Cryptography Foundations
  - Symmetric Cryptography
  - Asymmetric Cryptography

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

- Hashing
- Hybrid Crypto Systems
- Quantum Cryptography
- Advancements in Cryptography
- Attacking Weak Cryptography: Hashes, Keys, and Real-World Failures

- Module 5 - Vulnerability Scanning & Analysis
  - Understanding VA
  - Vulnerability Assessment Methodologies
  - Interpreting and Validating Vulnerabilities
  - Prioritizing Risks in VA
  - What is Patch Management?
  - Different Types of Patches
- Module 6 - Web and Application Attacks
  - OWASP Top 10 Explained
  - Bridging OWASP and CWE for Pen testers
  - API Top 10
- Module 7 - Exploitation and Post-Exploitation
  - Exploitation Basics
  - Exploit Frameworks in Action
  - Post-Exploitation Fundamentals
  - Pivoting and Lateral Movement
  - Cloud Exploitation Basics
- Module 8 - Social Engineering
  - Social Engineering Concepts and Psychology
  - Phishing and Digital Deception
  - Pretexting and In-Person Tactics
  - USB Drops and Device Attacks
  - Social Engineering Tools and Payloads
  - Case Studies and Field Operations
- Module 9 - Wireless Pen testing
  - Wi-Fi Recon and Enumeration
  - Wi-Fi Tools
  - Sniffing
  - Authentication Attacks
  - Rogue AP
  - Wi-Fi Exploits

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 Assessment
- Module 10 - Reporting & Ethics
  - The Role of Reporting in Ethical Hacking
  - Writing Effective Reports
  - Ethics in Ethical Hacking
  - Professional Development and Accountability
- Lab 0 - Lab Setup
  - Recording IPs and Logging into the VMs
  - Research
- Lab 1 - Identifying Hacker Personas
  - Case Studies
- Lab 2 - Threat Actor Research & Mapping
  - Investigation
- Lab 3 - Create a Pentest Proposal
  - Simulated Engagement Roleplay
- Lab 4 - Mapping CIA and AAA to Real-World Incidents
  - Incident 01 - Tesla Data Leak via Insider Threat
  - Incident 02 - Pegasus Airlines AWS Misconfiguration
  - Incident 03 - Schneider Electric Ransomware Attack
- Lab 5 - Exploring Access Control Models in Windows
  - Setup Users, Groups, and Folders
  - Apply DAC (Discretionary Access Control)
  - Apply RBAC (Role-Based Access Control)
  - Test Access Locally
- Lab 6 - Classifying Security Controls
- Lab 7 - Hacker Lifecycle Alignment + Recon Tools
- Lab 8 - Passive vs. Active Recon
  - Passive recon
  - Active recon
- Lab 9 - WHOIS, Google Dorking, Shodan
  - Whois lookup
  - Google Dorking
  - Shodan
  - Using previous documented data
- Lab 10 - DNS & SMB Enumeration
  - DNS Enumeration

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

- SMB Enumeration
- Lab 11 - Nmap & Basic Scripting
  - Basic Nmap Scan
  - Nmap Scripting Engine (NSE)
  - Bash Scripting
- Lab 12 - Cryptography
  - Hashing Data of all Sorts
  - The Basics of Cryptographic Algorithms
  - Using Bitlocker
  - Shredding Files
- Lab 13 - Risk Management and Vulnerability Assessment
  - Internet Research for CVE
  - Perform an Internal Vulnerability Assessment
  - Perform a Vulnerability Assessment Online
  - Vulnerability Scanning with Nessus Essentials server
- 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 - Advanced Vulnerability and Exploitation Techniques
  - Metasploitable Fundamentals
  - Metasploit Port and Vulnerability Scanning
  - Client-side attack with Metasploit
  - Using Workspaces in Metasploit
- Lab 16 - Wireless Security - Optional
  - Cracking WPA2 using AirCrack-ng
  - Cracking WPA2 using Wifite

REQUIREMENTS:

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

Suggested prerequisites:

- Participation in Mile2's C)SP - Certified Security Principles training
- 12 months of IT Experience
- 12 Months of Networking Experience

Difficulty level



CERTIFICATE:

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

This course will help prepare you for the Certified Professional Ethical Hacker CPEH 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)PEH training held in Compendium CE will receive a free CPEH Certified Professional Ethical Hacker 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