

Description:

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. Therefore, you can



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.



Annual Salary Potential \$80,077 AVG/year

Key Course Information	Modules/Lessons	Hands-On Labs
<p>Live Class Duration: 5 Days</p> <p>CEUs: 40</p> <p>Language: English</p> <p>Class Formats Available:</p> <ul style="list-style-type: none"> Instructor Led Self-Study Live Virtual Training <p>Suggested Prerequisites: (any one of the following)</p> <ul style="list-style-type: none"> Mile2's C/SP 12 months of IT Experience 12 Months of Networking Experience 	<p>Module 01: Introduction to Ethical Hacking</p> <p>Module 02: Cybersecurity Foundation</p> <p>Module 03: Reconnaissance & Enumeration</p> <p>Module 04: Cryptography</p> <p>Module 05: Vulnerability Scanning & Analysis</p> <p>Module 06: Web and Application Attacks</p> <p>Module 07: Exploitation and Post-Exploitation</p> <p>Module 08: Social Engineering</p> <p>Module 09: Wireless Pentesting</p> <p>Module 10: Reporting & Ethics</p>	<p>Lab 01: Identifying Hackers</p> <p>Lab 02: Threat Actor Research</p> <p>Lab 03: Create a Pentest Proposal</p> <p>Lab 04: Mapping CIA and AAA</p> <p>Lab 05: Exploring Access Control Models in Windows</p> <p>Lab 06: Classifying Security Cntrls</p> <p>Lab 07: Hacker Lifecycle Alignment + Recon Tools</p> <p>Lab 08: Passive vs. Active Recon</p> <p>Lab 09: WHOIS, Google Dorking, Shodan</p> <p>Lab 10: DNS & SMB Enumeration</p> <p>Lab 11: Nmap & Basic Scripting</p> <p>Lab 12: Cryptography</p> <p>Lab 13: Risk Management and Vulnerability Assessment</p> <p>Lab 14: OWASP TOP 10</p> <p>Lab 15: Advanced Vulnerability and Exploitation Techniques</p> <p>Lab 16: Wireless Security</p>

Upon Completion

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

Who Should Attend

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

Accreditations



Exam Information

The Certified Professional Ethical Hacker exam is taken online through 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.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

- 1) Pass the most current version of the exam for your respective existing certification
- 2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at

www.mile2.com.

Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options



Detailed Outline:

Module 00 – Course Introduction

Module 01: Introduction to Ethical Hacking

- Section 01: What is Ethical Hacking?
- Section 02: Threat Actors and Motivations
- Section 03: Hacker mindsets and methodologies
- Section 04: Rules of Engagement and Professional Conduct
- Section 05: Ethical Dilemmas and Gray Areas
- Section 06: Career Foundations

Module 02: Cybersecurity Foundation

- Section 01: Core Cybersecurity Principles
- Section 02: Security Architecture Fundamentals
- Section 03: Essential Security Controls
- Section 04: Security Governance and Policy
- Section 05: Applying Controls and Architecture in Testing
- Section 06: Risk, Compliance, and Controls

Module 03: Reconnaissance & Enumeration

- Section 01: Passive vs Active Reconnaissance
- Section 02: Practical Recon Tools
- Section 03: Enumeration Techniques
- Section 04: Applied Recon: Nmap, Scripting, and Enumeration
- Section 05: Practice Scenarios and Reporting
- Section 06: Capstone & Reflection

Module 04: Cryptography

- Section 01: Cryptography Foundations
- Section 02: Symmetric Cryptography
- Section 03: Asymmetric Cryptography
- Section 04: Hashing
- Section 05: Hybrid Crypto Systems
- Section 06: Quantum Cryptography
- Section 07: Advancements in Cryptography
- Section 08: Attacking Weak Cryptography: Hashes, Keys, and Real-World Failures

Module 05: Vulnerability Scanning & Analysis

- Section 01: Understanding VA
- Section 02: Vulnerability Assessment Methodologies
- Section 03: Interpreting and Validating Vulnerabilities
- Section 04: Prioritizing Risks in VA
- Section 05: What is Patch Management?
- Section 06: Different Types of Patches

Module 06: Web and Application Attacks

- Section 01: OWASP Top 10 Explained
- Section 02: Bridging OWASP and CWE for Pen testers
- Section 03: API Top 10

Module 07: Exploitation and Post-Exploitation

- Section 01: Exploitation Basics
- Section 02: Exploit Frameworks in Action
- Section 03: Post-Exploitation Fundamentals
- Section 04: Pivoting and Lateral Movement
- Section 05: Cloud Exploitation Basics

Module 08: Social Engineering

- Section 01: Social Engineering Concepts and Psychology
- Section 02: Phishing and Digital Deception
- Section 03: Pretexting and In-Person Tactics
- Section 04: USB Drops and Device Attacks
- Section 05: Social Engineering Tools and Payloads
- Section 06: Case Studies and Field Operations

Module 09: Wireless Pen testing

- Section 01: Wi-Fi Recon and Enumeration
- Section 02: Wi-Fi Tools
- Section 03: Sniffing
- Section 04: Authentication Attacks
- Section 05: Rogue AP
- Section 06: Wi-Fi Exploits
- Section 07: Threat Assessment

Module 10: Reporting & Ethics

- Section 01: The Role of Reporting in Ethical Hacking
- Section 02: Writing Effective Reports
- Section 03: Ethics in Ethical Hacking
- Section 04: Professional Development and Accountability

Labs:

Lab 00: Lab Setup

- Section 01: Recording IPs and Logging into the VMs
- Section 02: Research

Lab 01: Identifying Hacker Personas

- Section 01: Case Studies

Lab 02: Threat Actor Research & Mapping

- Section 01: Investigation

Lab 03: Create a Pentest Proposal

- Section 01: Simulated Engagement Roleplay

Lab 04: Mapping CIA and AAA to Real-World Incidents

- Section 01: Incident 01 - Tesla Data Leak via Insider Threat
- Section 02: Incident 02 - Pegasus Airlines AWS Misconfiguration
- Section 03: Incident 03 - Schneider Electric Ransomware Attack

Lab 05: Exploring Access Control Models in Windows

- Section 01: Setup Users, Groups, and Folders
- Section 02: Apply DAC (Discretionary Access Control)
- Section 03: Apply RBAC (Role-Based Access Control)
- Section 04: Test Access Locally

Lab 06: Classifying Security Controls

- Section 01: Classify the Security Controls

Lab 07: Hacker Lifecycle Alignment + Recon Tools

Section 01: Hacker Lifecycle Alignment + Recon Tools

Lab 08: Passive vs. Active Recon

Section 01: Passive recon

Section 02: Active recon

Lab 09: WHOIS, Google Dorking, Shodan

Section 01: Whois lookup

Section 02: Google Dorking

Section 03: Shodan

Section 04: Using previous documented data

Lab 10: DNS & SMB Enumeration

Section 01: DNS Enumeration

Section 02: SMB Enumeration

Lab 11: Nmap & Basic Scripting

Section 01: Basic Nmap Scan

Section 02: Nmap Scripting Engine (NSE)

Section 03: Bash Scripting

Lab 12: Cryptography

Section 01: Hashing Data of all Sorts

Section 02: The Basics of Cryptographic Algorithms

Section 03: Using Bitlocker

Section 04: Shredding Files

Lab 13: Risk Management and Vulnerability Assessment

Section 01: Internet Research for CVE

Section 02: Perform an Internal Vulnerability Assessment

Section 03: Perform a Vulnerability Assessment Online

Section 04: Vulnerability Scanning with Nessus Essentials server

Lab 14: OWASP TOP 10

- Section 01: Setup
- Section 02: A01: Broken Access Control
- Section 03: A02: Cryptographic Failures
- Section 04: A03: Injection
- Section 05: A05: Security Misconfiguration
- Section 06: A06: Vulnerable Components
- Section 07: A07: Authentication Failures
- Section 08: A09: Logging Failures
- Section 09: A10: Server-Side Request Forgery

Lab 15: Advanced Vulnerability and Exploitation Techniques

- Section 01: Metasploitable Fundamentals
- Section 02: Metasploit Port and Vulnerability Scanning
- Section 03: Client-side attack with Metasploit
- Section 04: Using Workspaces in Metasploit

Lab 16: Wireless Security - Optional

- Section 01: Cracking WPA2 using AirCrack-ng
- Section 02: Cracking WPA2 using Wifite