

## Description:

The Mile2 Certified Penetration Testing Engineer (CPTe) is an advanced, hands-on certification course for cybersecurity professionals ready to move beyond foundational ethical hacking into real-world penetration testing. The course teaches the full testing lifecycle, including scoping, reconnaissance, exploitation, post-exploitation, lateral movement, evasion, threat simulation, purple team collaboration, and business-focused reporting.



CPTe prepares students to assess modern enterprise environments such as traditional networks, cloud systems, Active Directory, Entra ID, Microsoft 365, web applications, APIs, and mobile applications. Students learn how to validate vulnerabilities safely, analyze attack paths, document evidence, and communicate technical findings as business risk. The course is ideal for those preparing for roles such as penetration tester, security engineer, red team operator, offensive security analyst, or security consultant.



## Annual Salary Potential \$119,895 AVG/year as of April 2026

Source note: ZipRecruiter lists the U.S. average salary for a penetration tester at approximately \$119,895 per year as of April 2026.

Completion of Mile2 provided training and/or education is not required to achieve any Mile2 certification.

Key Course Information	Modules/Lessons	Hands-On Labs
<p><b>Live Class Duration:</b> 5 Days</p> <p><b>CEUs:</b> 40</p> <p><b>Language:</b> English</p> <p><b>Class Formats Available:</b></p> <ul style="list-style-type: none"> <li>Instructor Led</li> <li>Self-Study</li> <li>Live Virtual Training</li> </ul> <p><b>Suggested Prerequisites:</b></p> <ul style="list-style-type: none"> <li>Mile2 C)PEH or equivalent knowledge</li> <li>12 months of Networking Experience</li> <li>Sound Knowledge of TCP/IP</li> <li>Basic Knowledge of Linux</li> <li>Microsoft Security experience</li> </ul>	<p><b>Module 01:</b> Penetration Testing Methodologies</p> <p><b>Module 02:</b> Advanced Recon &amp; Attack Surface Mapping</p> <p><b>Module 03:</b> Exploitation Techniques (Local &amp; Remote)</p> <p><b>Module 04:</b> Post-Exploitation &amp; Lateral Movement</p> <p><b>Module 05:</b> Cloud &amp; Active Directory Exploitation</p> <p><b>Module 06:</b> Evasion &amp; Payload Crafting</p> <p><b>Module 07:</b> Web, API &amp; Mobile Attacks</p> <p><b>Module 08:</b> Threat Simulation &amp; Attack Chains</p> <p><b>Module 09:</b> Purple Team Collaboration</p> <p><b>Module 10:</b> Reporting &amp; Business Risk Analysis</p>	<p><b>Lab 00:</b> Introduction to Pen Testing Setup</p> <p><b>Lab 01:</b> Pre-Engagement Planning</p> <p><b>Lab 02:</b> External Reconnaissance &amp; Attack Surface Mapping</p> <p><b>Lab 03:</b> Exploitation Techniques</p> <p><b>Lab 04:</b> Lateral Movement</p> <p><b>Lab 05:</b> Active Directory Recon and Attacks</p> <p><b>Lab 06:</b> C2 and Evasion</p> <p><b>Lab 07:</b> Web and API Attacks</p> <p><b>Lab 08:</b> Purple Team Collaboration</p> <p><b>Lab 09:</b> Final Report Assembly &amp; Professional Review</p>

## 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.

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

## 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.

## Accreditations



## Exam Information

The Certified Penetration Testing Engineer 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 Options

- 1) Submit CEUs and Purchase Certification Renewal
  - a. Earn and submit 60 CEUs over three years in your Mile2 account.
  - b. Purchase Certification Renewal
- 2) Retake Current Certification Exam

## 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](http://www.mile2.com).

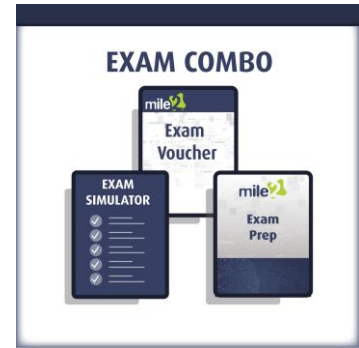
**Question:** Are all courses available as self-study courses?

**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



## Course Overview:

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.

## Detailed Outline:

### **Module 01: Penetration Testing Methodologies**

- Section 01: Pen Test Phases
- Section 02: Scoping and Legal Boundaries
- Section 03: OWASP Testing Framework

### **Module 02: Advanced Recon & Attack Surface Mapping**

- Section 01: Recon Philosophy & Objectives
- Section 02: DNS, Subdomains, and Certificates
- Section 03: OSINT & Metadata Intelligence
- Section 04: Tech Stack & Service Fingerprinting
- Section 05: Mapping the Attack Surface

### **Module 03: Exploitation Techniques (Local & Remote)**

- Section 01: Understanding Exploitation Process
- Section 02: Modern Exploitation Techniques and Shell Management
- Section 03: Payload Execution & Stability

### **Module 04: Post-Exploitation & Lateral Movement**

- Section 01: Credential Harvesting & Token Abuse
- Section 02: Scanning, Pivoting & Routing Through Compromised Hosts
- Section 03: Lateral Movement Techniques
- Section 04: Persistence Mechanisms
- Section 05: Hiding Persistence and Cleanup

### **Module 05: Cloud & Active Directory Exploitation**

- Section 01: Enterprise Identity and AD Basics for Attackers
- Section 02: Local Priv Esc → Domain Admin Escalation Paths
- Section 03: Azure/M365 Exploitation – Initial Access to Persistence
- Section 04: Hybrid Identity Exploitation Paths (AD Connect, Entra Sync)
- Section 05: Real-World Kill Chain Examples (Hybrid Pathways)

## **Module 06: Evasion & Payload Crafting**

- Section 01: EDR & AV Evasion Fundamentals
- Section 02: Crafting Payloads with Caution
- Section 03: Obfuscation and Execution Techniques
- Section 04: Frameworks & Modern C2 Delivery
- Section 05: Red Team Tradecraft for Evasion Success

## **Module 07: Web, API & Mobile Attacks**

- Section 01: OWASP Top 10 Deep Dive
- Section 02: Advanced API Testing
- Section 03: Mobile App Exploitation (Android/iOS)
- Section 04: Web Shells and Post-Exploitation via Web
- Section 05: Defense Evasion in Web Contexts

## **Module 08: Threat Simulation & Attack Chains**

- Section 01: Threat Simulation Fundamentals
- Section 02: Planning and Scoping an Attack Chain
- Section 03: Chaining Techniques – From Access to Impact
- Section 04: Threat Simulation Tools and Frameworks
- Section 05: Communication, Debriefing, and Lessons Learned

## **Module 09: Purple Team Collaboration**

- Section 01: Introduction to Purple Teaming
- Section 02: Building a Purple Team Program
- Section 03: Adversary Emulation in Purple Teams
- Section 04: Detection Engineering and Alert Tuning
- Section 05: Purple Team Exercises – Real World to Lab
- Section 06: Continuous Improvement and Lessons Learned

## **Module 10: Reporting & Business Risk Analysis**

- Section 01: Reporting for Technical and Executive Audiences
- Section 02: Prioritizing Findings Based on Business Risk
- Section 03: Communicating Attack Paths and Exposure Chains
- Section 04: Mapping Findings to Frameworks and Controls
- Section 05: Strategic Debriefing and Executive Communication
- Section 06: Improving the Reporting Lifecycle

## Detailed Lab Outline:

### **Lab 00: Introduction to Pen Testing Setup**

Section 01: Recording IPs and Logging into the VMs

Section 02: Connect Windows VMs to AD

### **Lab 01: Pre-Engagement Planning**

Section 01: Engaging the Client: Defining the Engagement

Section 02: The Results: Scope, Constraints, and Professional Judgment

Section 03: Setting Up Dradis: Formalizing the Engagement

### **Lab 02: External Reconnaissance & Attack Surface Mapping**

Section 01: Understanding External Visibility (Passive Recon)

Section 02: Identify Exposed Services and Technologies

Section 03: Active Recon and Surface Mapping

Section 04: Correlation and Attack Path Visualization

Section 05: Reporting & Professional Documentation

### **Lab 03: Exploitation Techniques**

Section 01: Authenticated Access & Job Abuse

Section 02: Post-Exploitation Evidence Collection

Section 03: Privilege Escalation via Docker Abuse

Section 04: Credential Harvesting & Internal Recon

Section 05: Persistence

Section 06: Reporting in Dradis CE

### **Lab 04: Lateral Movement**

Section 01: Lateral Movement via Jenkins Agents

Section 02: Recon the Internal Network

Section 03: Pivoting Through DB Connection

### **Lab 05: Active Directory Recon and Attacks**

Section 01: BloodHound & SharpHound

Section 02: Vertical Privilege Escalation

Section 03: DCSync

**Lab 06: C2 and Evasion**

Section 01: Create an Evasive Payload

**Lab 07: Web and API Attacks**

Section 01: Getting WebGoat up and Running

Section 02: Application Reconnaissance & Attack Surface Mapping

Section 03: Authorization Testing: Object Access & IDOR

Section 04: API Authorization Failures

Section 05: Session & Identity Trust Abuse

Section 06: Token-Based Authentication Failures

Section 07: Client-Side Controls as an Attack Enabler

**Lab 08: Purple Team Collaboration**

Section 01: Detection Engineering Baseline

Section 02: Controlled Adversary Simulation

Section 03: Detection Validation & Gap Analysis

Section 04: Mitigation & Hardening Discussion

Section 05: Bypass Techniques

Section 06: Incident Response & Timeline Reconstruction

**Lab 09: Final Report Assembly & Professional Review**

Section 01: Report Quality Audit

Section 02: Strengthening Remediation Guidance

Section 03: Executive Summary Creation

Section 04: Exporting the Final Report

Section 05: Final Professional Review Checklist