



## Certified Penetration Testing Engineer<sup>TM</sup>

### DATOS CLAVE

**Nombre del curso:**  
CPTeEngineer<sup>TM</sup>

**Duración:** 5 días

**Pre-requisitos:**

- \* Un mínimo de 12 meses de experiencia en redes
- \* Conocimientos técnicos de TCP/IP
- \* Conocimiento de software de Microsoft
- \* Network+, Microsoft, Security+
- \* Conocimiento básico de Linux es esencial

**Materiales:**

- \* Manual de Estudiante
- \* Manual de Lab de Estudiante
- \* Software y Herramientas

**Examen de Certificación:**

- \* CPTE - Certified Pen Testing Engineer<sup>TM</sup>
- \* CEH - Certified Ethical Hacker<sup>TM</sup>
- \* CPEH - Certified Professional hacker<sup>TM</sup>
- \* OSCP - Offensive Security Certified Professional<sup>TM</sup>

**Track de Certificaciones:**

- \* CPTE - Certified Pen Testing Engineer<sup>TM</sup>
- \* CPTC - Certified Pen Testing Consultant<sup>TM</sup>
- \* CDFF - Certified Digital Forensics Examiner<sup>TM</sup>

### BENEFICIOS DEL CURSO

Aquellos que finalicen satisfactoriamente el curso de Certified Penetration Testing Engineer habrán obtenido el conocimiento de la seguridad en el mundo real que les permitirá reconocer vulnerabilidades, explotar las debilidades en los sistemas y ayudar a protegerse de las amenazas. Los graduados del curso habrán aprendido el arte del Ethical Hacking, pero, con el nivel profesional (Penetration Testing).

### RESUMEN DEL CURSO

Las bases del curso de CPTeEngineer están sentadas firmemente en la experiencia de campo de nuestro grupo internacional de consultores en el campo de Penetration Testing. Los instructores de Mile2 mantienen vigente su experiencia practicando lo que enseñan; creemos que un énfasis equitativo entre la teoría y la experiencia en el mundo real es esencial para una transferencia de conocimiento efectiva para el estudiante.

El curso de CPTeEngineer presenta la información basado en 5 elementos clave del Pen Testing: Obtención de Información, Escaneo, Enumeración, Explotación y Reporte; las últimas vulnerabilidades serán descubiertas usando estas técnicas reales y comprobadas. Este curso también mejora las habilidades de negocios necesarias para identificar oportunidades de protección, justificar actividades de evaluación y optimizar los controles de seguridad de forma apropiada para las necesidades del negocio y de esta forma reducir los riesgos. Mile2 va más allá de simplemente enseñar como "hackear" como fueron las clases típicas disponibles antes de la revolucionaria metodología de Mile2.

Nuestro curso esta desarrollado con base en principios y métodos usados por los hackers maliciosos, SIN EMBARGO, nuestro foco son las pruebas de penetración profesionales y la evaluación de los activos de información.

### AL CONCLUIR

Los estudiantes del CPTeEngineer estarán listos para tomar con confianza el examen de certificación de CPTeEngineer. El examen de certificación es presentado vía web sobre la plataforma MACS (Mile2 Assesment & Certification System), en línea y en inglés. Consta de 100 preguntas de selección múltiple y una duración de 2 horas. Se obtiene la aprobación del examen con un resultado superior al 75%. El curso ofrece laboratorios propietarios actualizados que son fruto de la investigación y desarrollo de profesionales líderes en seguridad de alrededor del mundo.



## MÓDULOS DEL CURSO

Módulo 0: Introducción al Curso  
Módulo 1: Logística de Negocios y Técnica del Pen Testing  
Módulo 2: Regulaciones del Sector Financiero  
Módulo 3: Obtención de Información  
Módulo 4: Detección de Sistemas Activos  
Módulo 5: Enumeración  
Módulo 6: Evaluación de Vulnerabilidades  
Módulo 7: Malware, Troyanos y BackDoors  
Módulo 8: Hacking de Windows  
Módulo 9: Hacking de Unix/Linux  
Módulo 10: Técnicas de Explotación Avanzadas  
Módulo 11: Pen Testing de Redes Inalámbricas  
Módulo 12: Redes, Sniffing e IDS  
Módulo 13: Inyectando la Base de Datos  
Módulo 14: Atacando Tecnologías Web  
Módulo 15: Escribiendo Reportes  
Apéndice 1: Lo Básico  
Apéndice 2: Fundamentos de Linux  
Apéndice 3: Controles de Acceso  
Apéndice 4: Protocolos  
Apéndice 5: Criptografía  
Apéndice 6: Economía y Leyes

## OBJETIVOS DE LOS ESCENARIOS DE LABORATORIO

Ésta es una clase interactiva al máximo donde usted pasará más de 20 horas realizando laboratorios en lugar de pasar mucho tiempo instalando cientos de herramientas. Nuestro foco está en el modelo de Pen Testing. Se enseñarán los últimos métodos y herramientas de Pen Testing. Los laboratorios cambian semanalmente según se encuentran nuevos métodos. Se usarán diferentes herramientas desde un GUI hasta la línea de comandos. Según como se avanza con los ataques estructurados, se trabaja y enseñan herramientas tanto para Windows como Linux.