

## Certified Professional Ethical Hacker

### DATOS CLAVE

#### Nombre del curso:

C)PEH

#### 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 deseable en Linux, no es indispensable

#### Materiales:

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

#### Examen de Certificación:

- CPTS: Certified Pen Testing Specialist (Thompson Prometric – Globally)

#### Track de Certificaciones:

- CPTE - Certified Pen Testing Engineer<sup>TM</sup>
- CPTS - Certified Pen Testing Specialist
- CDFE - Certified Digital Forensics Examiner<sup>TM</sup>

Puntaje de aprobación: 70%

## BENEFICIOS DEL CURSO

Los estudiantes que tomen el curso de Certified Professional Ethical Hacker habrán obtenido conocimiento real del mundo de la seguridad que los hará capaces de reconocer vulnerabilidades, exponer debilidades de sistemas y ayudar a protegerlos contra amenazas. Los estudiantes del curso habrán aprendido el arte del Ethical Hacking, pero, con un enfoque profesional (Penetration Testing).

## RESUMEN DEL CURSO

CPEH es desarrollado por manos expertas en metodologías de Prueba de Penetración utilizadas por nuestro grupo de consultores en vulnerabilidades internacionales. El curso CPEH presenta información sobre las últimas vulnerabilidades y defensas. Este curso también reafirma las habilidades de negocio necesarias para identificar oportunidades de protección, justificar actividades de pruebas y optimizar los controles de seguridad apropiados para las necesidades de cada negocio, con la finalidad de reducir riesgos de negocio. Nuestros cursos van más allá de simplemente enseñar a “Hackear”. Nuestros cursos son desarrollados basándose en principios y metodología usados por hackers maliciosos, pero enfocados en pruebas de penetración profesional y asegurando los activos de información.

## AL CONCLUIR

Los estudiantes de CPEH serán capaces de tomar el examen de CPTS en la plataforma Thompson Prometric (recomendado). Los estudiantes disfrutarán de un curso a profundidad, constantemente actualizado para mantenerlo incorporado al, siempre cambiante, mundo de seguridad.

## Certified Professional Ethical Hacker

### OBJETIVOS DE LOS ESCENARIOS DE LABORATORIOS

Este es un curso intensivo con metodología “hands on” que se enfoca en el modelo de Pruebas de Penetración. En él se encontrará las herramientas y métodos más recientes para Pruebas de Penetración. Los laboratorios cambian semanalmente conforme nuevos métodos aparecen. Utilizará muchas y variadas herramientas GUI para línea de comando. Como el trabajo es a través de estructuras de ataque, cubrimos herramientas de sistemas Windows y Linux.

### MÓDULOS DEL CURSO

**Módulo 1: Security Fundamentals**

**Módulo 2: Access Controls**

**Módulo 3: Protocols**

**Módulo 4: Network Attack and Defense**

**Módulo 5: Cryptography**

**Módulo 6: Economics and Law**

**Módulo 7: Reconnaissance**

**Módulo 8: Scanning and Enumeration**

**Módulo 9: Gaining Access/Exploitation**

**Módulo 10: Maintaining Access**

**Módulo 11: Covering your tracks**

**Módulo 12: Malware**

**Módulo 13: Buffer Overflows**

**Módulo 14: Password cracking attacks**

**Módulo 15: Denial of service**

**Módulo 16: Attacking web technologies and database**

**Módulo 17: Attacking wireless devices**

Los cursos de Mile2 están acreditados por NSA CNSS 4011-4016, en Homeland's Security National, NICCS training schedule, preferido por el FBI Nivel 1-3.

