C)PEH™
CERTIFIED PROFESSIONAL ETHICAL HACKER

Certified Professional Ethical Hacker™

DATOS CLAVE

Nombre del curso: PEH

Duración: 5 días

Idioma: Español

Formato: Aula con instructor

Pre-requisitos:

* Un mínimo de 12 meses de experiencia en tecnologías de red
* Buen conocimiento de TCP/IP
* Conocimiento en hardware
* Conocimiento de paquetería Microsoft
* Network+, Microsoft Security+
* Conocimiento deseable en Linux, no es indispensable

Material del estudiante:

* Cuaderno de Trabajo del Alumno
* Manual de Referencia del Alumno
* 3 Dvd's con software + herramientas

Examen de Certificación:

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

Track de Certificaciones:

* CPTS – Certified Pen Testing Specialist™
* CPTE - Certified Pen Testing Engineer™
* CDFE - Certified Digital Forensics Examiner™

BENEFICIOS DEL CURSO

Los estudiantes que tomen el curso 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 de las amenazas. Los estudiantes aprenderán el arte del Hackeo Ético, pero con enfoque profesional (Penetration Testing).

DESCRIPCIÓN DEL CURSO

PEH es desarrollado por manos expertas en metodologías de Prueba de Penetración utilizadas por nuestro grupo de consultores en vulnerabilidades internacionales. El curso PEH 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 PEH serán capaces de tomar el examen 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.

OBJETIVOS DE LOS ESCENARIOS DE LABORATORIO

Este es un curso intensivo con metodología “hands on” que se enfoca en el modelo de Pruebas de Penetración. En él 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.

CNSS

pt™ PENETRATION TESTING

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 Databases

Módulo 17: Attacking Wireless Devices