C)PTC™
CERTIFIED PENETRATION TESTING CONSULTANT

Certified Penetration Testing Consultant™

DATOS CLAVE

Nombre del curso: CPTCv3

Duración: 4 días

Idioma: Español

Formato: Aula con instructor

Pre-requisitos:

* Conocimiento de CPTE, GIAC o equivalente
* Un mínimo de 24 meses de experiencia en tecnología de redes
* Conocimientos técnicos de TCP/IP
* Conocimiento de hardware
* Experiencia como Profesional de Soporte o Consultor

Materiales:

* Cuaderno y Manual de Estudiante
* Software y Herramientas

Examen de Certificación:

* CPTC – Examen práctico

Track de Certificaciones:

* CPTE - Certified Pen Testing Engineer™
* CPTC - Certified Pen Testing Consultant™
* CSWAE – Certified Secure Web Application Engineer™

OBJETIVOS DEL PROGRAMA CPTC

El programa de "Certified Penetration Testing Consultant" está diseñado para profesionales de la seguridad de TI y para Administradores de Redes TI (IT Network Administrators) interesados en realizar pruebas de penetración en grandes infraestructuras de redes, similares a las de las grandes redes corporativas, de proveedores de servicios y de empresas de telecomunicaciones. En vez de enfocarse en la penetración a nivel de sistemas operativos, este programa cubre técnicas sobre cómo atacar y evitar la sub-infraestructura de las redes y sus protocolos. El entrenamiento comienza con temas básicos de análisis y captura de paquetes y mediante el uso de herramientas comunes y continúa con los vectores de segunda capa, y los ataques de capa 3; incluyendo "stacks" (cúmulos de información abstracta) IPv4 y IPv6, ataques con protocolos de ruteo (OSPF, BGP, etc.) y después se brinca a ataques a nivel del proveedor de servicios relacionados con MPLS comunes, cómo usar relevos y pivotes, etc., ataques VPN que incluyen la suite de protocolo IPSEC, ataques SSL y finalmente cubre también técnicas de evasión e implementación NIDS/NIPS. Al término de cada módulo, los participantes serán capaces de practicar los conocimientos adquiridos con ejercicios de laboratorio que han sido específicamente preparados para complementar los materiales teóricos.

AL CONCLUIR

Al concluir el programa, el Consultor Certificado en Pruebas de Penetración tendrá los conocimientos fundamentales para administrar y ejecutar un plan de penetración. La designación de "Consultor" está relacionada con la amplitud y profundidad de conocimiento requerido para administrar un proyecto que involucre a varias personas, administrar las expectativas del cliente y entregar una auditoría de controles de seguridad que es comprensiva, bien documentada y ética.

OBJETIVOS DE LOS ESCENARIOS DE LABORATORIO

El examen para certificación como Consultor de Penetración tiene una duración de 6 horas, es un examen práctico en el que el estudiante tendrá que realizar una Evaluación de Vulnerabilidad (Vulnerability Assessment) y una prueba total de penetración en dos IPs. Después se le darán 60 días para entregar un reporte escrito de la prueba de penetración, reporte que será analizado por nuestro equipo de expertos. Al estudiante se le pedirá que identifique por lo menos el 80% de las vulnerabilidades y después realizar pruebas manuales para comprobar que éstas son legítimas. El reporte deberá ser escrito en forma profesional. Este examen se pasa o se reprueba.

CNSS

pt™ PENETRATION TESTING

EXAMEN PARA CERTIFICACIÓN COMO CONSULTOR

Este es un curso interactivo intensivo. Los estudiantes dedicarán del orden de 20 horas haciendo ejercicios de laboratorio que les permitirán experimentar un laboratorio real de penetración. Los laboratorios comienzan con simples actividades y evolucionan con procedimientos más sofisticados. En los laboratorios, los estudiantes contarán con guías detalladas que contendrán pantallas, comandos que deberán ser introducidos y que guiarán paso a paso a los estudiantes. Los estudiantes podrán usar variedades de herramientas de última generación de Penetración (GUI y líneas de comandos, Windows y Linux) conforme avanzan en la metodología probada de Mile2 . Nuestros clientes pueden tener la seguridad de que nuestros laboratorios estarán siempre actualizados con los últimos métodos que surjan en el mundo de la seguridad.

MÓDULOS Y LABORATORIOS DEL CURSO

Módulo 0: Introducción al CPTC
Módulo 1: Captura de Paquetes
Módulo 2: Ataques de capa 2
Módulo 3: Ataques de capa 3 en infraestructuras soportadas por CISCO
Módulo 4: Pivotes y Relays
Módulo 5: Ataques IPv6
Módulo 6. Ataques VPN
Módulo 7: Venciendo al SSL
Módulo 8: Evasión IDS/IPS

Lab 1: Trabajando con archivos capturados
Lab 2: Ataques de capa 2
Lab 3: Atacando protocolos de Ruteo
Lab 4: Utilizando máquinas Pivote
Lab 5: Ataques IPv6
Lab 6: Ataques VPN
Lab 7: Venciendo al SSL – Des-encriptando tráfico y ataques del "Man-in-the-Middle"
Lab 8: NIDS/NIPS