C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

mile2® CYBER SECURITY CERTIFICATIONS

Certified Penetration Testing Engineer

DATOS CLAVE

Nombre del curso:

CPTEngineer™

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™
- CEH - Certified Ethical Hacker™
- CPEH - Certified Professional hacker™
- OSCP - Offensive Security Certified Professional™

Track de Certificaciones:

- CPTE - Certified Pen Testing Engineer™
- CPTC - Certified Pen Testing Consultant™
- CDFE - Certified Digital Forensics Examiner™

Puntaje de aprobación: 70%

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 CPTEngineer 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 CPTEngineer presenta la información basado en 5 elementos clave del PenTesting: 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 está 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 CPTEngineer estarán listos para tomar con confianza el examen de certificación de CPTEngineer. 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.

C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

mile2® CYBER SECURITY CERTIFICATIONS

Certified Penetration Testing Engineer

OBJETIVOS DE LOS ESCENARIOS DE LABORATORIOS

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 os ataques estructurados, se trabaja y enseñan herramientas tanto para Windows como Linux.

MÓDULOS DEL CURSO

Module 0: Course Overview
Module 1: Logistics of Pen Testing
Module 2: Linux Fundamentals
Module 3: Information Gathering
Module 4: Detecting Live Systems
Module 5: Enumeration
Module 6: Vulnerability Assessments
Module 7: Malware Goes Undercover
Module 8: Windows Hacking
Module 9: Hacking UNIX/Linux
Module 10: Advanced Exploitation Techniques
Module 11: Pen Testing Wireless Networks
Module 12: Networks, Sniffing and IDS
Module 13: Injecting the Database
Module 14: Attacking Web Technologies
Module 15: Project Documentation

Lab 1: Getting Set Up
Lab 2: Linux Fundamentals
Lab 3:Information Gathering
Lab 4: Detecting Live Systems
Lab 5: Reconnaissance
Lab 6: Vulnerability Assessment
Lab 7: Malware
Lab 8: Windows Hacking
Lab 9: UNIX/Linux Hacking
Lab 10: Advanced Vulnerability and Exploitation
Lab 11: Attacking Wireless Networks
Lab 12: Network Sniffing and IDS
Lab 13: Database Hacking
Lab 14: Hacking Web Applications
Lab A5: Cryptography
Post Class Lab: Core Impact

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.

CNSS — NIST National Institute of Standards and Technology — NICCS National Initiative for Cybersecurity Careers and Studies

IAS™ INFORMATION ASSURANCE SERVICES | PT™ PENETRATION TESTING | DR™ DISASTER RECOVERY | GS™ GENERAL SECURITY | SC™ SECURE CODING | VBP™ VIRTUALIZATION BEST PRACTICES | WS™ WIRELESS SECURITY | CF™ COMPUTER FORENSICS