

Certified Penetration Testing Engineer

Código: CPTE-001

Propuesta de Valor: SEGURIDAD INFORMÁTICA

Duración: 40 Horas



Las bases del curso de CPTEngineer están sentadas firmemente en la experiencia de campo de un 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 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.



AUDIENCIA

Este curso está dirigido a:

- Pen Testers
- Ethical Hackers
- Auditores de redes
- Profesionales de seguridad cibernética
- Evaluadores de Vulnerabilidad
- Administradores de Seguridad Cibernética
- Gerentes IS



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



OBJETIVOS

- Desarrollar estándares de evaluación adecuados de la industria con excelentes procedimientos y arreglos
- Evaluaciones de vulnerabilidad
- Recopilación de información
- Pruebas de penetración de redes inalámbricas
- Detección de sistemas vivos



CERTIFICACIÓN DISPONIBLE

- Certificación oficial de **COGNOS**.



CONTENIDO

1. MODULO 0 - COURSE OVERVIEW
2. MODULO 1 - BUSINESS & TECHNICAL LOGISTICS OF PEN TESTING
3. MODULO 2 - LINUX FUNDAMENTALS
4. MODULO 3 - INFORMATION GATHERING
5. MODULO 4 - DETECTING LIVE SYSTEMS
6. MODULO 5 - ENUMERATION
7. MODULO 6 - VULNERABILITY ASSESSMENTS
8. MODULO 7 - MALWARE GOES UNDERCOVER
9. MODULO 8 - WINDOWS HACKING
10. MODULO 9 - HACKING UNIX/LINUX
11. MODULO 10 - ADVANCED EXPLOITATION TECHNIQUES
12. MODULO 11 - PEN TESTING WIRELESS NETWORKS
13. MODULO 12 - NETWORKS, SNIFFING AND IDS
14. MODULO 13 - INJECTING THE DATABASE
15. MODULO 14 - ATTACKING WEB TECHNOLOGIES
16. MODULO 15 - PROJECT DOCUMENTATION
17. MODULO 16 - SECURING WINDOWS W/ POWERSHELL*

★ BENEFICIOS

- Al finalizar el curso, los estudiantes del CPTEngineer estarán listos para tomar con confianza el examen de certificación de CPTEngineer.