Certified Penetration Testing Consultant

Código: CPTC-001

Propuesta de Valor: SEGURIDAD INFORMÁTICA

Duración: 40 Horas

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.

AUDIENCIA

Este curso está dirigido a:

- Oficiales de seguridad de IS
- Gerentes / Administradores de Seguridad Cibernética
- Probadores de penetración
- Ethical Hackers
- Auditores

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

OBJETIVOS

- 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.

CERTIFICACIÓN DISPONIBLE

- Certificado emitido por **COGNOS**
- Este curso lo prepara para el examen **CPTC**

CONTENIDO

1. FORMACIÓN DEL EQUIPO DE PRUEBAS DE PENETRACIÓN

2. AUTOMATIZACIÓN NMAP

3. PROCESO DE EXPLOTACIÓN

4. FUZZING WITH SPIKE

5. DESBORDAMIENTO SIMPLE DEL BÚFER

6. DESBORDAMIENTO DEL BÚFER DE WINDOWS BASADO EN PILA

7. SEGURIDAD Y EXPLOTACIÓN DE APLICACIONES WEB

8. LINUX STACK SMASHING & SCANNING

9. ALEATORIZACIÓN DEL DISEÑO DEL ESPACIO DE DIRECCIONES DE LINUX

10. PROTECCIÓN CONTRA EXPLOITS DE WINDOWS

11. CÓMO MOVERSE SEH ASLR

12. INFORME DE PRUEBA DE PENETRACIÓN REDACCIÓN

BENEFICIOS

- Al finalizar el curso, los participantes tendran un conocimiento solido de los procedimientos de prueba e informes que los preparan para los roles de alta gerencia dentro de un sistema de ciberseguridad.