PEN-200 Pruebas de Penetración con Kali Linux (OSCP)

Código: PKL-001

Propuesta de Valor: OTROS CURSOS DE CAPACITACIÓN TECNOLÓGICA

Duración: 40 Horas

La prueba de penetración con Kali Linux (PEN-200) es el curso fundamental en Offensive Security. Los nuevos en OffSec o las pruebas de penetración deben comenzar aquí. Este curso de piratería ética en línea es a su propio ritmo. Introduce herramientas y técnicas de prueba de penetración a través de la experiencia práctica. PEN-200 entrena no solo las habilidades, sino también la mentalidad requerida para ser un probador de penetración exitoso. Los estudiantes que completen el curso y aprueben el examen obtienen la codiciada certificación Offensive Security Certified Professional (OSCP).

AUDIENCIA

- Profesionales de Infosec en transición a las pruebas de penetración.
- Pentesters que buscan una certificación líder en la industria.
- Profesionales de seguridad.
- Administradores de red.
- Otros profesionales de la tecnología.

PRE REQUISITOS

- Sólido conocimiento de las redes TCP / IP.
- Experiencia razonable en administración de Windows y Linux.
- Familiaridad con las secuencias de comandos básicas de Bash y / o Python.

OBJETIVOS

Adquirir conocimientos en:

- Usar técnicas de recopilación de información para identificar y enumerar objetivos que ejecutan varios sistemas operativos y servicios.
- Escribir scripts y herramientas básicos para ayudar en el proceso de prueba de penetración.
- Analizar, corregir, modificar, compilar y portar código de explotación pública.

- Realización de ataques remotos, locales de escalada de privilegios y del lado del cliente.
- Identificación y explotación de vulnerabilidades de XSS, inyección SQL e inclusión de archivos en aplicaciones web.
- Aprovechando las técnicas de tunelización para pivotar entre redes.
- Habilidades creativas de resolución de problemas y pensamiento lateral.

CERTIFICACIÓN DISPONIBLE

- Certificado oficial de **COGNOS**.
- Este curso lo prepara para el examen: **OffSec Certified Professional (OSCP)**.

CONTENIDO

1. PRUEBAS DE PENETRACIÓN CON KALI LINUX: INTRODUCCIÓN GENERAL AL CURSO

2. INTRODUCCIÓN A LA CIBERSEGURIDAD

3. ESTRATEGIAS DE APRENDIZAJE EFECTIVAS

4. REDACCIÓN DE INFORMES PARA PROBADORES DE PENETRACIÓN

5. RECOPILACIÓN DE INFORMACIÓN

6. ESCANEO DE VULNERABILIDADES

7. INTRODUCCIÓN A LAS APLICACIONES WEB

8. ATAQUES COMUNES A APLICACIONES WEB

9. ATAQUES DE INYECCIÓN SQL

10. ATAQUES DEL LADO DEL CLIENTE

11. LOCALIZACIÓN DE HAZAÑAS PÚBLICAS

12. ARREGLANDO EXPLOITS

13. EVASIÓN ANTIVIRUS

14. ATAQUES DE CONTRASEÑA

15. ESCALADA DE PRIVILEGIOS DE WINDOWS

16. ESCALADA DE PRIVILEGIOS DE LINUX

17. TÚNEL AVANZADO

18. EL MARCO DE METASPLOIT

19. INTRODUCCIÓN Y ENUMERACIÓN DE ACTIVE DIRECTORY

20. ATACAR LA AUTENTICACIÓN DE ACTIVE DIRECTORY

21. MOVIMIENTO LATERAL EN ACTIVE DIRECTORY

22. ENSAMBLANDO LAS PIEZAS

23. ESFORZARSE MÁS: LOS LABORATORIOS

BENEFICIOS

Al finalizar el curso, tendrás conocimientos en:

- Introducción a las últimas herramientas y técnicas de piratería.
- Capacitación de los expertos detrás de Kali Linux.
- Aprenda el método y la mentalidad de "Inténtelo más duro".
- Obtenga la certificación OSCP líder en la industria.