



Curso: Metodologías de Test de intrusión y Hacking ético (Presencial / e-Learning)

1. NORMAS DE REFERENCIA

- OSSTMM – Metodología de Testeo de la Seguridad de Código Abierto.
- OWASP – Proyecto Abierto de Seguridad de Aplicaciones Web.
- ISSAF – Framework de la seguridad en los sistemas de información.

2. DESCRIPCIÓN DEL CURSO

Objetivos:

- El objetivo del curso es que el alumno se familiarice con las metodologías de test de intrusión y conozca las amenazas y riesgos existentes en Internet para aplicar las medidas oportunas que posibiliten minimizar los riesgos.

Duración: 40 horas

Modalidades: Presencial y e-Learning

El curso e-Learning estará alojado en el servidor Web de START UP.

Se incluye un servicio de tutorías mediante el correo electrónico de forma que ante cualquier duda, el alumno pueda obtener una respuesta rápida y concreta de especialistas en la materia.

Contenidos:

1. Presentación presencial del curso y su temario.
2. Recopilación de información:
 - A través de medios técnicos: DNS, Nmap, Whois, Dig, ...
 - A través de medios no técnicos: News, foros, 'Googling', etc.
3. Network Mapping
 - Uso de la información obtenida anteriormente para confeccionar la infraestructura de red.
4. Información de vulnerabilidades:
 - Detección de vulnerabilidades del Software
5. Análisis y monitorización de ficheros del log sistema.
 - Interpretando logs en el sistema y el servidor web
6. Metodología OWASP
 - Descripción de contramedidas según metodología OWASP para aplicaciones web.



3. EJERCICIOS DEL CURSO

- Examinar el Sistema de Nombre de Dominio:
 - Buscar información del registrador y el bloque de IP
 - Comprobar servidores autoritativos
 - Comprobar la existencia de DNS inversos
 - Comprobar la presencia en listas negras de SPAM
- Buscar históricos de los sistemas
- Búsqueda en sitios de indexación
- Sistema de Correo Electrónico:
 - Enumeración de cuentas de correo
 - Análisis de las cabeceras SMTP
- Investigar los DNS
 - Realizar transferencias de zona
 - Realizar transferencias de zona con diccionario
- Escáner de Puertos TCP
- Escáner de Puertos UDP
- Identificación de Servicios
- Descubrimiento ARP
- Identificar el perímetro de la red
- Realizar un escáner FIN/ACK
- Identificación Pasiva de Sistemas Operativos
- Identificación Activa de Sistemas Operativos
- Análisis de Paquetes HTTP
- Análisis de Paquetes ICMP
- Enumeración de Sistemas
- Identificación de vulnerabilidades
- Escáner automatizado de vulnerabilidades
- Pruebas de testeo para aplicaciones web

4. EXPERIENCIA

Realizamos cursos presenciales y e-learning de diversos niveles en el ámbito de la seguridad de la información en las Cámaras de Comercio de Oviedo, Álava, Tenerife y Cantabria. Algunos de nuestros clientes son Telecable, Urazca, Camerfirma, etc....

5. PRESUPUESTO

e-Learning: 400 € por alumno.

Presencial: 7200 €. Están incluidos todos los gastos para la impartición del curso a un número de 20 alumnos en las instalaciones del cliente.