



TALLERES HACKING ETICO

Reconocimiento y Enumeracion, Sniffers y Key loggers, Exploracion de Puertos, Escaneo y Análisis de Vulnerabilidades.

La permanente exposición al riesgo de robo, Extravió, alteración o delitos sobre la información confidencial de las empresas, situando a estas en una posición bastante delicada y critica, por lo que se hace imperioso conocer las herramientas y metodologías utilizadas por los mismos hackers y posibles atacantes, para poder contrarrestarlas eficazmente.

El curso de Ethical Hacking brinda un amplio conocimiento y practica real en equipos de las más actuales herramientas y técnicas de ataque y defensa, permitiéndonos consecuentemente actuar profesionalmente sobre el tema. Tiene un enfoque totalmente práctico, basado en distintos tipos de ataques y sobre diversos entornos.

¿A quien esta dirigido?:

Especialmente a Profesionales de áreas de Sistemas, Consultores de Tecnología, Auditores Internos y Externos de Sistemas, Profesionales, Administradores y Responsables de Seguridad Informática.

Material:

Al finalizar el entrenamiento se entregará un CD con las presentaciones, manuales, las herramientas utilizadas durante el seminario y herramientas adicionales complementarias.

Certificado:

Se entregaran certificados de asistencia a todos los participantes.

Duración:

3 Días (24 hrs), sobre los cuales usted podrá practicar todas las configuraciones de seguridad requeridas.

Horario:

De 09:00 a 18:00

Requisitos:

Conocimientos Básicos de Tecnología.

Seminario taller 100% Practico, un participante por computador



Temario a desarrollar

- **Tráfico de Red**→ Análisis de los campos de cabeceras en protocolos TCP/IP. Reconocimiento de tráfico malicioso, lectura de tráfico. Análisis e interpretación de archivos RAW. Revisión documentos RFC 791 y RFC 793. Módulo de nivelación.
- **Reconocimiento y Enumeración**→ Técnicas de mapeo de redes, subnetting, conocimiento por oscuridad, herramientas para conocer registros DNS (A, MX, NS), enumeración de servicios, listado de directorios, estructura de sitios e infraestructura de red, reconocimiento de maquinas por sistema operativo, protocolos y aplicaciones. Empleo de estándares internacionales reconocidos como OSSTM
- **Sniffers y Keyloggers**→ Interceptación de tráfico. Captura de contraseñas. Captura de tráfico de mensajería Instantánea. Explicación en Capa II, tráfico de diferentes plataformas e infraestructuras
- **Exploración de Puertos**→ Interrogación de Puertos TCP y UDP. Técnicas de escaneo. Interrogación maliciosa. Redirección de puertos, conexiones remotas
- **Escaneo y Análisis de Vulnerabilidades**→ Exploración de Bugs, sistema operativo, vulnerabilidades conocidas. Relación bugs-exploits. Búsqueda y Análisis de diferentes vulnerabilidades
- **Troyanos**→ Revisión y Ejecución de Troyanos, Técnicas y prácticas de esteganografía y troyanización de archivos jpg, mp3, avi, divx y archivos de texto. Enbedido y unión de ejecutables en otros tipos. Código malicioso.

Recursos: Cada participante contara con un computador conectado a la red, en donde realizaran sus prácticas.

Por ser un seminario práctico los cupos son limitados.