

Education Center – Temarios Detallados

Taller Ethical Hacking – OSINT (Open Source Intelligence) or “The Low Hanging Fruit”

Introducción:

En un análisis de seguridad, uno de los primeros pasos que un Security Tester debe dar, es el de reconocer de manera pasiva toda la información disponible de su objetivo, claro está, las mismas acciones son llevadas a cabo también por potenciales intrusos para el desarrollo de una efectiva estrategia de ataque.

Sabemos que información de la organización está disponible de manera pública?

En un mundo WEB 2.0 Sabemos cuánta de esta información es aparentemente inútil por sí misma pero muy útil si se la relaciona con otra información pública?

Estamos listos para enfrentarnos a una manipulación más eficiente de datos en la inminente Web 3.0?

Objetivo:

El objetivo de este taller es el de brindar de una manera práctica los conceptos y las herramientas necesarias para que de manera proactiva, pueda llevar a cabo en su organización análisis periódicos orientados a identificar y eliminar información pública que yace en buscadores, portales, foros, blogs, redes sociales, grupos, listas de correo y otros sitios que permitan a un tercero sacar partido de la misma.

Dirigido a:

Oficiales de Seguridad de la Información, Administradores de Seguridad, Administradores de Redes, Desarrolladores con orientación a la Seguridad, Consultores en Seguridad de la Información, Auditores.

Metodología:

Orientada a la práctica, en la cual mediante laboratorios hands-on se aprenden las técnicas utilizadas en las diferentes técnicas de Information Gathering. La práctica está también enfocada a generar un ambiente colaborativo y de trabajo en grupos.

Habilidades que desarrollará el participante:

El participante desarrollará habilidades prácticas en la utilización de herramientas de análisis tanto a nivel particular como general de las mismas, todo esto dentro de un marco metodológico y de ética profesional que caracterizan este tipo de prácticas.

Requisitos del Participante:

- Conocimientos básicos sobre Aplicaciones
- Conocimientos básicos sobre Infraestructura IT
- Capacidad de lectura y autoestudio.

Material a Entregar:

- Presentaciones impresas y en formato digital
- Set de CDs compuestos por las herramientas utilizadas durante la capacitación.

Instructores:

Ezequiel Sallis - CISSP, CEH, MBCI

Claudio B. Caracciolo - CEH, MCSE, ASE, CATE

Ambos instructores cuentan con más de **12 años** de experiencia en la práctica de análisis de seguridad en las principales empresas nacionales e internacionales. En ambos casos han brindado más de **50 capacitaciones** y más de **60 conferencias** relacionadas al tema a lo largo de su carrera.

Duración:

La capacitación tendrá una duración de 8hs.

Temario:

Introduccion

- Inteligencia - Algunas Definiciones
- OSINT de que se trata?
- OSINT en que se basa?
- OSINT porque?

Casos Practicos

- Information Gathering (Old Style)
- GOOSINT (Google Hacking)
- OSINT 2.0
- Metadata
- All in One

Conclusiones Finales