Open Source Intelligence

CC5325 - Taller de Hacking Competitivo
Diego Vargas

Contenidos

- Introducción a OSINT
- Fuentes de información
- Herramientas de búsqueda
- Demo

Introducción a OSINT

Definición

Wikipedia:

> Es una metodología multifactorial (cualitativa y cuantitativa) de recolección, análisis y toma de decisiones sobre datos de fuentes disponibles de forma pública para ser utilizados en un contexto de inteligencia.

Uso en la realidad

El OSINT puede ser una de las habilidades más importantes para ciertas actividades relacionadas a la seguridad.

Entrega información relevante sobre un objetivo en particular, la cual puede ser utilizada para enumerar o realizar fuerza bruta, como también para explotar vulnerabilidades.

Fuentes de Información

Categorías de Flujo de Información

- Medios de comunicación
- Internet
- Datos gubernamentales
- Publicaciones profesionales y académicas
- Datos comerciales
- Literatura gris

Internet

Hoy en día casi todo está en internet, por lo que las otras categorías pueden ser un poco redundantes o innecesarias. Sin embargo, se pueden volver muy necesarias si realizan trabajos como investigación forense o policial.

Herramientas de Búsqueda

Motores de búsqueda

Búsqueda de información general mediante strings o parámetros de restricción.

- Google/DuckDuckGo Search
- Google/DuckDuckGo Dorks
- Github Search
- Wikipedia

TheHarvester

Utiliza motores de búsqueda para encontrar IPs, subdominios y direcciones de correo asociadas a un dominio en particular.

Útil para hacer una búsqueda rápida de recursos conocidos públicamente de una empresa.

Shodan

Motor de búsqueda que permite encontrar tipos específicos de computadores o dispositivos conectados a internet.

Capaz de encontrar dispositivos inteligentes, como termostatos, cámaras, sensores, luces, cerraduras digitales, entre muchos otros.

Have I Been Pwned

Repositorio de contraseñas filtradas en internet, junto a correos asociados.

Permite consultar (de manera segura) si cierto correo o cierta contraseña ha sido parte de una filtración.

Demo

Herramientas

- theHarvester
- Google/DuckDuckGo
- Shodan
- HaveIBeenPwned