Las**herramientas de OSINT**(Inteligencia de Fuentes Abiertas) son recursos técnicos utilizados en internet para acceder a información «escondida». Para Eric Schmidt, exdirector de Google, casi el 100% de la información en línea no es visible para los motores de búsqueda frecuentes.

Sin estas herramientas, el proceso de búsqueda, recopilación y análisis de información para esclarecer un tema consume tiempo y recursos. ¿Ejecutas una búsqueda infructuosa en internet? Las técnicas que te mostramos a continuación pueden ayudarte a encontrar las fuentes y datos correctos, correlacionarlos y utilizarlos cuando quieras.

**Herramientas  de OSINT más utilizadas**

Según [Informe de la RSE](https://sgp.fas.org/crs/intel/RL34270.pdf) del Congreso estadounidense, la Inteligencia de Fuentes Abiertas se genera a partir de la información pública difundida en internet. Estos datos son reunidos, explotados eficazmente y puestos a la orden de los usuarios, a través de **herramientas de OSINT** como las siguientes:

**Maltego**

Este *software* de Java simplifica y agiliza cualquier investigación. Actualmente, Maltego garantiza el acceso a casi 60 fuentes de datos, ayudando a visualizar aproximadamente 1 millón de valores en un gráfico. Genera resultados de fácil comprensión gracias a una potente herramienta de visualización.



Puedes conectar tus bases de datos públicas y cargar fuentes de información manualmente. Cuando hayas realizado la carga en el programa, puedes elegir cómo visualizar la información y ajustar los gráficos según tus necesidades, agregando pesos y notas.  Entre sus características están:

* Fue diseñado por Paterva.
* Es una aplicación Java.

Tu publicidad aquí

* Se encuentra integrado en kali Linux entre otras distribuciones.

Esta herramienta permite la creación y desarrollo de huellas digitales efectivas de cualquier objetivo en internet.

**SEON**

SEON es, básicamente, una herramienta para la prevención de fraude que verifica más de 50 señales de redes sociales *online*. Esto se realiza a partir de un número telefónico, una dirección IP o un correo electrónico.



Claro que siempre es posible buscar en la Red Social objetivo directamente, introduciendo manualmente un nombre en Facebook, Twitter, Instagram o Linkedin; pero, por motivos de escalabilidad (a través de API), es mucho más sencillo y fluido utilizar una herramienta como SEON, la cual facilita:

* La colocación de barreras para [estafadores](https://ciberinseguro.com/como-hacer-phishing/) sin recursos para tener perfiles falsos.
* La recopilación de huellas digitales de los usuarios.
* La obtención de una gran cantidad de información sobre el usuario, usando sus redes sociales.

SEON es compatible con casi 40 redes sociales y plataformas *web*. Puede instalarse como una extensión de Google Chrome o utilizar el servicio mediante la Interfaz de Programación de Aplicaciones (API). Una de sus ventajas es la opción de conocer las puntuaciones de riesgo de cada transacción.

**TheHarvester**

TheHarvester es una de las más versátiles **herramientas de OSINT** para conseguir una dirección de *email*, un DNS o un subdominio a partir de un dominio.



Se vale de comandos para obtener datos públicos, ya sea de manera pasiva o activa. La obtención de información pasiva significa que no existe una interacción con el objetivo. Los datos se obtienen utilizando los motores de búsqueda integrados al *software*.

El modo activo implica aplicar «fuerza bruta» al DNS o eliminar los *screenshots* de los subdominios localizados. La interacción con el objetivo es directa.

**Shodan**

Es un poderoso motor de búsqueda con gran atractivo para los piratas informáticos; facilita la detección de múltiples dispositivos conectados a la red, mediante filtros: activos en IoT, cámaras *web*, *routers*, ordenadores y mucho más. Estos filtros afinan cada búsqueda, reduciendo el rango de acción; por ejemplo: buscar por ciudad, puerto abierto, fechas, país u otros criterios.



Básicamente, genera información sobre activos expuestos en línea y su nivel de vulnerabilidad. Algunos de sus casos de uso frecuente son:

* Verificación de contraseñas predeterminadas.
* Dispositivos con visor *Virtual Network Computing* (VNC).
* Uso del puerto RDP (puerto TCP 3389) para comprobar activos disponibles.

Es de gran utilidad para los expertos en ciberseguridad que buscan determinar la exposición de contraseñas y otros datos de sus clientes ante los *[ciberdelincuentes](https://ciberinseguro.com/como-hackear-una-cuenta-de-instagram-facebook-tiktok-twitter/)*.

**Have I Been Pwnd?**

Este programa ayuda a detectar filtraciones de credenciales en cuentas creadas con un determinado correo electrónico. Y no solo eso, con HIBP? puedes conocer otros correos electrónicos, números telefónicos y contraseñas revelados a partir de esta filtración.



De manera concisa, esta herramienta inteligente le sirve al usuario para saber si sus datos personales fueron expuestos sin su autorización. Al introducir el correo o una contraseña en el software, es posible conocer si han sido hackeados y si están siendo usados por alguien más.

Este proyecto de *Open Source* creado por Troy Hunt, ha integrado más de 200 millones de datos a su ya extensa base de datos, para consulta pública.

**Spiderfoot**

Esta técnica OSINT ha sido desarrollada especialmente para especialistas en investigación e inteligencia. Es muy utilizada por profesionales en ciberseguridad que mantienen un seguimiento continuo de activos o que monitorizan posibles ataques.



Esta aplicación tiene acceso automático a más de 100 fuentes de información pública en tiempo real. Así, se puede acceder a correos electrónicos, nombres, direcciones, dominios y mucha información requerida para una investigación. ¿Cómo utilizarla? Te contamos brevemente:

* Puedes alojarla como un proyecto de código abierto.
* Conseguir la versión alojada, totalmente administrada por Spiderfoot.
* Usarla como una herramienta integrada a kali Linux.

Si adquieres la versión alojada recibirás la cooperación del equipo de Spiderfoot y establecerás correlaciones en tu investigación. Aquí todos los módulos  y funciones ya están instalados y configurados.

**¿Cuál es la herramienta OSINT para ti?**

El alcance de las técnicas y **herramientas de OSINT** exhibe un universo de gran amplitud. Si te adentras en el mundo de la Inteligencia de Código Abierto verás que no todos los proyectos se ajustan a tus necesidades.

Por eso, debes definir para qué lo necesitas. ¿Buscas pistas para mejorar tu *marketing* digital? ¿Investigas un crimen? ¿Quieres fortalecer tu página *web*? ¿Deseas saber si tu información financiera y personal fue filtrada? Delimitar claramente estos parámetros te permitirá elegir la herramienta idónea y sacarle un mayor provecho.