OSINT

Open Source INTelligence

Juan Gualberto Gutiérrez

¿Qué es eso de OSINT?

Llamamos OSINT al conocimiento recopilado a partir de fuentes de acceso público, ojo público no quiere decir gratuito, también es posible *"comprar"* esa información de manera **lícita**. El proceso incluye la búsqueda, selección y adquisición de la información, así como un posterior procesado y análisis de la misma con el fin de obtener conocimiento útil y aplicable en distintos ámbitos.

¿Mande? ¿Me lo explicas con otras palabras...? 😆

OSINT

OSINT se refiere a la recopilación, análisis y uso de información de fuentes públicas y accesibles a todos. En otras palabras, OSINT se trata de obtener información útil y valiosa de fuentes de información que están disponibles para cualquiera, como redes sociales, sitios web, noticias, blogs y otros recursos en línea.

OSINT

La información recopilada a través de OSINT se utiliza comúnmente para investigaciones, seguridad, inteligencia empresarial, análisis de mercado, entre otros fines. OSINT es una herramienta muy útil para la recopilación de información en la era digital, ya que hay una gran cantidad de información disponible en línea y se pueden utilizar técnicas de búsqueda y análisis para extraer información relevante.

Inteligencias en el ámbito militar y de servicios de información

OSINT es una de las disciplinas de recolección de inteligencia, como también lo son:

1. HUMINT: Hace referencia a la inteligencia recogida a partir de una persona en un espacio en cuestión.
2. GEOINT: Inteligencia geoespacial.
3. IMINT: Inteligencia a partir de imágenes.
4. MASINT: Inteligencia de medidas de señales, como pueden ser: nucleares, electromagnéticas, ópticas, de radar

Fuentes abiertas como por ejemplo:

- Medios de comunicación: revistas, periódicos, radio, etc.
- Información pública de fuentes gubernamentales.
- Foros, redes sociales, blogs, wikis, etc.
- Conferencias, simposios, «papers», bibliotecas online, etc.

Utilidad del OSINT:

- Conocer la reputación online de un usuario o empresa.
- Realizar estudios sociológicos, psicológicos, lingüísticos, etc.
- Auditoria de empresas y diferentes organismos con el fin de evaluar el nivel de privacidad y seguridad.
- Evaluar tendencias de mercados.
- Identificación y prevención de posibles amenazas en el ámbito militar o de la seguridad nacional.
- Como aspecto negativo, es utilizado por cibercriminales para lanzar ataques APT y «Spear Phishing».

Fases investigación:

Fases investigación:

1. **Dirección y planificación**: es la fase en la que se establecen todos los requerimientos que se deben cumplir, es decir, aquellas condiciones que deben satisfacerse para conseguir el objetivo o resolver el problema que ha originado el desarrollo del sistema OSINT.
2. **Adquisición**: consiste en especificar, a partir de los requisitos establecidos, las fuentes de interés que serán recopiladas. Hay que tener presente que el volumen de información disponible en Internet es prácticamente inabordable por lo que se deben identificar y concretar las fuentes de información relevante con el fin de optimizar el proceso de adquisición.

Problemas principales en OSINT

- **Demasiada información**: como ya se ha puesto de manifiesto, la cantidad de información pública disponible en Internet es más que notable. Es por ello, que se debe realizar un proceso muy exhaustivo a la hora de identificar y seleccionar las fuentes de información de interés que van a ser recopiladas, y que posteriormente servirán para la generación de inteligencia. El hecho de utilizar un catálogo extenso de fuentes conlleva obviamente un mayor gasto a la hora de implementar el sistema, y en el caso de no tener disponibles los recursos necesarios, provoca una significativa ralentización del mismo.
- **Fiabilidad de las fuentes**: es importante valorar previamente

Antes de comenzar...

Como investigador OSINT, es importante que tomes medidas para proteger tu privacidad y seguridad en línea, especialmente si estás recopilando información sensible o investigando temas delicados.

Siempre debes proteger tu identidad y siempre debemos evitar infringir la ley en tus actividades de investigación.

Recomendaciones

- **Máquinas virtuales**: Una de las mejores prácticas es trabajar en una máquina virtual, ya que te permite crear un ambiente aislado del sistema operativo principal de tu ordenador. De esta manera, puedes instalar software específico para OSINT sin correr el riesgo de infectar tu sistema principal con malware o virus.

Recomendaciones

- **VPN**: Una VPN (Red Privada Virtual) es una herramienta que te permite navegar de forma anónima y segura en internet. Es especialmente útil si estás investigando desde una ubicación pública, como una biblioteca o una cafetería, ya que encripta tus datos y oculta tu dirección IP.

Recomendaciones

- **Cuentas ficticias**: Si estás investigando en redes sociales, es recomendable que utilices cuentas ficticias para evitar que tus actividades sean rastreadas hasta tu cuenta personal. Sin embargo, es importante que sigas los términos de servicio de la red social y no infrinjas la ley.

Recomendaciones

- **Gestor de contraseñas**: Cuando creas muchas cuentas es importante recordar las contraseñas, es recomendable usar un gestor no online para ello.

Recomendaciones

- **Herramientas de OSINT**: Hay muchas herramientas disponibles para OSINT, como motores de búsqueda especializados, herramientas de análisis de redes sociales y de búsqueda de información. Es recomendable que investigues y pruebes diferentes herramientas para encontrar las que mejor se adapten a tus necesidades.

Recopilación de datos

Aunque hoy día existen plataformas o sistemas como Maltego o Leonardo que combinan herramientas de Big Data e Inteligencia Artificial para ayudar a comprender y seguir el rastro de la información de nuestras investigaciones, normalmente el investigador OSINT usa diferentes herramientas Web combinadas con otros script (normalmente en Python) de elaboración propia o específicos para el tipo de investigación.

Herramientas para Instagram

- instaloader
- instalooter
- toutatis
- Osintgram

Herramientas de usuario / correo electrónico

Existen multitud de herramientas como:

1. Sherlock
2. Holene
3. SocialScan
4. WhatsMyName
5. Email2Phone

Herramientas para analizar redes (CLI)

1. amass: Busca subdominios dentro del indicado.
2. TheHarvester:
3. Photon
4. Carbon14
5. EyeWhitness
6. Rastrea2r

Herramientas para investigar redes (Web)

- WiFi: Wigle: Permite buscar por SSID, BSSID, área, etc.
- Por IP: Shodan: La cuenta gratuita permite 100 búsquedas al mes. Nos permite ver puertos abiertos sin hacer escaneo activo. También se puede hacer consultas sencillas sin login así: http://https://beta.shodan.io/host/88.26.231.151 -en este momento esta es la IP del IES-.
- Reverse DNS: ViewDNS, ejemplo: https://viewdns.info/reverseip/?host=2.139.173.60
- Geolocalización: iplocation.net. Consulta varios servicios de geolocalización. Si lo probamos con la IP del centro, no termina de llegar con precisión a nuestra localización, pero se acerca

Google Dorks

- "término de búsqueda" Utiliza este para hacer una búsqueda exacta.
- OR busca esto o aquello. Este devolverá resultados relacionados con los dos términos o con ambos.
- AND buscar esto y aquello. Este solo devolverá resultados relacionados con los dos términos
- – Excluir un término o una frase de búsqueda.
- * Actúa como un comodín y encontrará cualquier palabra o frase.
- ( ) Agrupa múltiples términos u operadores para controlar cómo

Ejemplos prácticos de Google Dorks

- **intitle:index.of “Apache/*” “server at” site:.es**: Esto busca servidores Apache que muestran la versión en España. Vamos a encontrar muchos organismos públicos y Universidades.
- **intitle:"toshiba network camera – User Login"**: Da acceso a muchos grabadores o NVR abiertos a Internet.
- **"teléfono * * *" "dirección *" "e-mail" intitle:"curriculum vitae"**: Información personal sesible de muchas personas que tienen su CV expuesto en Internet.

Herramientas de Telegram

- Fuente: Awesome Telegram OSINT

Herramientas de Office 365

- PWC - Office365 Extractor

Herramientas búsqueda de código

- Grep.APP
- SourceGraph

Herramientas para investigar Proton Mail y VPN

- ProtOSINT