EasyChair Preprint

№ 13324

Proposal for the Integration of the OSINT SpiderFoot Tool with the OSSIM Security Information and Event Management System

Dariel González Robinson, Angel Alejandro Guerra Vilches and Heidy Rodríguez Malvarez

May 16, 2024

Propuesta para la integración de la herramienta OSINT SpiderFoot con el Sistema de Gestión de Eventos e Información de Seguridad OSSIM.

Dariel González Robinson
Universidad de las Ciencias Informáticas
Cuba
dgonzalezr@estudiantes.uci.cu

Angel Alejandro Guerra Vilches
Universidad de las Ciencias Informáticas
Cuba
angelagv@estudiantes.uci.cu

Heidy Rodríguez Malvarez
Universidad de las Ciencias Informáticas
Cuba
heidyrm@estudiantes.uci.cu

Resumen- **OSSIM Alienvault (Open Source Security Information Manager) es una plataforma de Administración de Eventos e Información de Seguridad (SIEM por sus siglas en inglés), gratuita y de código abierto que permite la detección de amenazas y anomalías en la seguridad de las redes y de las computadoras. SpiderFoot es una herramienta de automatización OSINT (Open Source Intelligence, por sus siglas en inglés) que se integra con diversas fuentes de datos y ofrece varios tipos de escaneos para recopilar información. El objetivo de esta investigación es proponer una posible integración de la herramienta SpiderFoot con OSSIM para automatizar el proceso de recopilación de información, utilizando la información recopilada tanto de fuentes internas, como externas.**

Palabras claves- **OSINT, SpiderFoot, SIEM, OSSIM, integración.**

Tipo de contenido: *Investigación en desarrollo.*

I. Introducción

Los ataques cibernéticos se han vuelto más severos y frecuentes, lo que requiere una nueva línea de defensas de seguridad para protegerse contra ellos. En opinión de [1], la naturaleza dinámica de las amenazas de nueva generación, que son evasivas, resistentes y complejas, hace que los sistemas de seguridad tradicionales tengan dificultades para detectarlas. El objetivo de las organizaciones es recopilar y compartir información sobre amenazas cibernéticas en tiempo real y luego convertirla en inteligencia de amenazas para prevenir ataques o, al menos, responder rápidamente de manera proactiva.

La minería de Inteligencia de Amenazas Cibernéticas (CTI por sus siglas en inglés) que descubre, procesa y analiza información valiosa sobre amenazas cibernéticas, está en auge. La cantidad de datos generados por el mundo interconectado actual es inconmensurable y gran parte de estos están disponibles públicamente, lo que significa que son accesibles para cualquier usuario, en cualquier momento, desde cualquier lugar de Internet. En este sentido, la Inteligencia de Fuente Abierta (OSINT) es un tipo de inteligencia que realmente se beneficia de esa naturaleza abierta al recopilar, procesar y correlacionar puntos de todo el Ciberespacio para generar conocimiento [2].

Mientras que el uso manual de técnicas OSINT puede ser suficiente para búsquedas básicas, herramientas como SpiderFoot automatizan el proceso de recopilación de información permitiendo a los usuarios realizar investigaciones más profundas y completas sin la necesidad de realizar tareas manuales tediosas.

Al aprovechar esta vasta fuente de información abierta, los sistemas SIEM se destacan como una poderosa herramienta de seguridad que ayuda a las organizaciones a detectar y analizar amenazas, así como a responder a ellas antes de que afecten las operaciones del negocio. OSSIM (Open Source Security Information Manager) es una solución integral.

Actualmente, al realizar los análisis forenses ante un incidente reportado en OSSIM, se toman los datos y se realizan búsquedas más profundas de forma manual. Este proceso es lento y poco efectivo ya que se realiza de forma reactiva e implica la presencia de personal especializado, por tanto, la integración de herramientas OSINT al SIEM OSSIM, permite que se recopile información de forma rápida y eficiente a través de diversas fuentes en línea.

Ante la problemática anteriormente expuesta se plantea como objetivo de la investigación: Proponer una posible integración de la herramienta SpiderFoot en el SIEM OSSIM para la recopilación de información externa desde fuentes de datos abiertas.

II. Contenido

Herramienta OSINT (SpiderFoot):

SpiderFoot[1] es una herramienta de automatización de Inteligencia de Fuente Abierta (OSINT) escrita en Python 3. Se integra con varias fuentes de datos disponibles y utiliza una variedad de módulos para el análisis de datos. Tiene un servidor web integrado para proporcionar una interfaz limpia e intuitiva basada en la web, pero también se puede utilizar completamente a través de la línea de comandos.

Las características clave de la herramienta SpiderFoot son:

- Motor de correlación configurable por YAML con 37 reglas predefinidas.
- Más de 200 módulos.
- Exportación CSV/JSON/GEXF.

[1] Disponible en https://github.com/smicallef/spiderfoot

- Exportación/importación de claves API.
- Back-end de SQLite para consultas personalizadas.
- Integración de TOR para la búsqueda en la Dark Web.
- Dockerfile para implementaciones basadas en Docker.
- Puede llamar a otras herramientas como DNSTwist, Whatweb, Nmap y CMSeeK.

SpiderFoot revisa automáticamente varias fuentes de datos públicos para recopilar información. Toma como posibles entradas una dirección IP, una subred, un nombre de dominio, una dirección de correo electrónico, un nombre de host, un nombre real o un número de teléfono. Basándose en la entrada del usuario para realizar un reconocimiento efectivo, selecciona los módulos a usar.

Dependiendo del nivel de búsqueda seleccionado por el usuario, Spiderfoot ofrece cuatro tipos de escaneos:

- Passive: recopila información sin interactuar con el objetivo.
- Investigate: realiza un escaneo básico para detectar malicia.
- Footprint: identifica la topología de red del objetivo y recopila información suficiente para investigaciones estándar.
- All: realiza un escaneo exhaustivo consultando todos los recursos posibles. Es ideal para investigaciones detalladas, pero requiere más tiempo.

Herramienta SIEM (OSSIM):

OSSIM es una plataforma de software SIEM, gratuita y de código abierto, desarrollada por AlienVault y basada en la distribución Debian Linux de 64 bits. Integra un conjunto de herramientas como Nmap, Nagios, Suricata, Nessus, OpenVAS, entre otras que le permiten ejecutar funciones como:

- Descubrimiento de activos
- Escaneo de vulnerabilidades
- Detección de amenazas y anomalías
- Monitoreo de red
- Inteligencia de seguridad

OSSIM tiene cuatro componentes principales como se muestra en la Figura 1: sensor, servidor, marco de referencia, y base de datos.

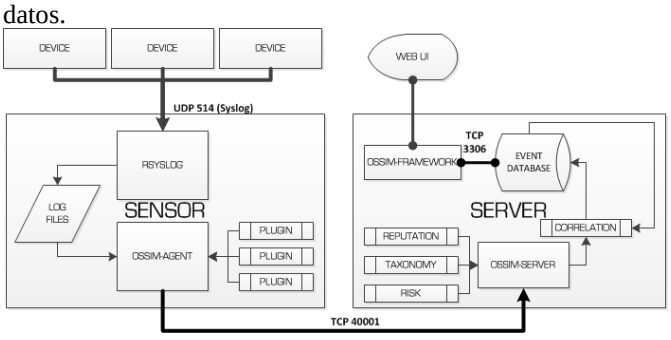

Fig. 1: Modelo de la arquitectura OSSIM. Fuente [3]

Cada componente se describe [3]:

El Sensor tiene dos partes. El servicio *rsyslog* recibe y almacena registros de dispositivos de red. El agente OSSIM analiza y normaliza estos registros y los envía al servidor.

El Servidor realiza funciones esenciales de SIEM como la agregación, evaluación de riesgos y correlación de eventos. También envía información de eventos a la base de datos para su almacenamiento.

El Marco de referencia (Framework) conecta y gestiona los componentes OSSIM y las herramientas de seguridad. También proporciona la interfaz web de administración del sistema.

La base de datos almacena eventos y datos de configuración del sistema.

Integración:

La solución propuesta se diseña con el objetivo de automatizar el proceso de recopilación de información, aprovechando la información de fuentes internas recopilada por los sensores de OSSIM, como de las fuentes externas recopiladas por SpiderFoot. Se considera una fuente interna a los componentes y sistemas dentro de la propia infraestructura de la empresa y una fuente externa a las fuentes públicas disponibles en línea.

El modelo estructural de la herramienta resultante se expone en la Figura 2. La herramienta SpiderFoot se instala junto con los componentes del servidor y el marco de trabajo del OSSIM.

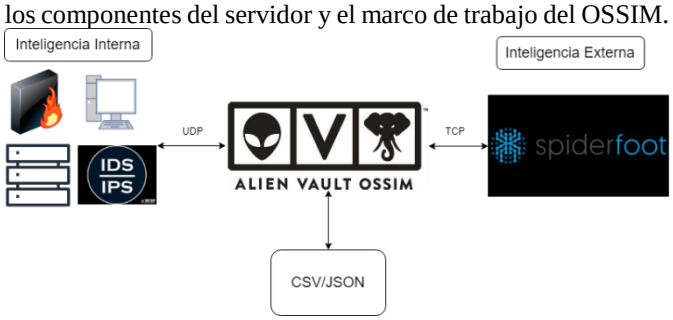

Fig. 2: Modelo de integración OSSIM-SpiderFoot.

Para el funcionamiento automatizado de la recopilación de los datos se tiene que ejecutar los siguientes pasos:

1. La creación de un script personalizado en OSSIM que se encargue de proporcionar como datos de entrada a SpiderFoot las direcciones IP, nombres de dominios u otra información relevante de las alertas que genera OSSIM. Varios módulos de SpiderFoot requieren una clave API para su funcionamiento. Al utilizar estos módulos, se autentica con las APIs correspondientes utilizando las claves proporcionadas para autenticar las solicitudes realizadas a la API REST de SpiderFoot. Para los módulos que no requieren estas claves, simplemente se ejecuta el script y este se encarga de realizar las peticiones de información necesarias.
2. La configuración de OSSIM para usar el script de manera automatizada cada vez que se genere una alerta, o manual cuando se desee consultar información externa. Esto puede implicar la modificación de las reglas de correlación de OSSIM o la configuración de acciones de respuesta.

OSSIM recopila registros de eventos de servidores y dispositivos de red, datos de tráfico de red de los switches y routers, y resultados de escaneo de vulnerabilidades de herramientas como Nessus o OpenVAS.

Una vez que OSSIM ha recopilado los datos, los correlaciona para identificar patrones y anomalías. Por ejemplo, si OSSIM detecta un gran número de intentos de inicio de sesión fallidos seguidos en un corto período de tiempo que provienen de la misma dirección IP o del mismo rango de direcciones IP,

correlaciona estos eventos y los reconoce como un posible ataque de fuerza bruta.

Basándose en la correlación de eventos, OSSIM genera alertas para informar a los administradores de seguridad sobre posibles amenazas. Estas alertas incluyen direcciones IP que se envían a través de la línea de comandos de forma automatizada a la herramienta SpiderFoot a través del script personalizado.

SpiderFoot recibe las direcciones IP y realiza su propio análisis. Esto puede incluir la recopilación de información adicional sobre las direcciones IP, la correlación de las direcciones IP con otras fuentes de datos y la generación de informes o alertas basados en los resultados del análisis.

Los resultados se muestran a través de la interfaz web donde se exportan en formatos CSV y JSON. Dependiendo de los resultados del análisis de la herramienta OSINT, se toman medidas adicionales como incluir la investigación más a fondo de las direcciones IP, la implementación de medidas de seguridad adicionales o la notificación a las autoridades pertinentes.

III. Conclusiones

La aplicación de técnicas de Inteligencia de Fuente Abierta (OSINT) en la seguridad cibernética, como se demuestra en esta investigación, abre un nuevo horizonte en la lucha contra las amenazas cibernéticas.

Al recopilar, procesar y correlacionar información de todo el Ciberespacio, se puede generar un conocimiento valioso que puede ser utilizado para prevenir y responder a amenazas cibernéticas de manera más efectiva.

Esta investigación también destaca la importancia de la automatización en la seguridad cibernética. Al automatizar el proceso de recopilación de información, las organizaciones pueden liberar recursos valiosos que pueden ser utilizados en otras áreas críticas de la seguridad cibernética.

Por otra parte, el valor de la colaboración entre diferentes herramientas y plataformas en la seguridad cibernética es muy importante. Al integrar SpiderFoot con OSSIM, se demuestra cómo diferentes herramientas pueden trabajar juntas para proporcionar una solución de seguridad más completa y robusta.

IV. **Referencias**

[1] N. Sun, M. Ding, J. Jiang, W. Xu, X. Mo, Y. Tai y J. Zhang, «Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives,» *IEEE Communications Survey & Tutorial*, vol. 25, p. 28, 05 mayo 2023.

[2] J. Pastor-Galindo, P. Nespoli, F. Gómez Mármol y G. Martínez Pérez, «The not yet exploited goldmine of OSINT: opportunities, open challenges and future trends,» *IEEE ACCESS*, vol. 8, p. 23, 9 Enero 2020.

[3] M. Alamanni, «OSSIM: a careful, free and always available guardian for your network,» *Linux Journal*, vol. 2014, nº 242, 02 junio 2014.

[4] Intel 471, «Attack surface documentation,» 2024. [En línea]. Available: https://intel471.com/attack-surface-documentation.