REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
TELEM@TICA
Revista Telem@tica. Vol. 11. No. 1, enero-abril, 2012, p. 11-19 ISSN 1729-3804

OSSIM, una alternativa para la integración de la gestión de seguridad en la red

Walter Baluja García[1], Cesar Camilo Caro Reina[2], Frank Abel Cancio Bello[3]

[1] ISPJAE, Ingeniero en Telecomunicaciones y Electrónica, Dr. C. Tec. walter@tesla.cujae.edu.cu

[2]ISPJAE. Estudiantes de 5to Año de Telecomunicaciones y Electrónica cesarcamilo.cr@fecrd.cujae.edu.cu

[3] ISPJAE, Ingeniero en Informática frankabel@tesla.cujae.edu.cu

RESUMEN / *ABSTRACT*

En la actualidad resulta cada vez más complicado mantenerse asegurado frente a los diferentes ataques que se pueden presentar en una red, lo cual resulta en una gestión de seguridad mucho más compleja para los administradores de red. Para cumplir con ese cometido los gestores utilizan un grupo de soluciones que permiten automatizar su trabajo, gestionando grandes volúmenes de información. El presente artículo realiza un breve resumen sobre los sistemas de Administración de Información y Eventos de Seguridad (SIEM por sus siglas en ingles), revisando sus principales características, y continua con la descripción del sistema OSSIM Alienvault, donde se muestran su arquitectura y componentes.

Palabras claves: Gestión, Seguridad, SIEM, OSSIM.

OSSIM, an alternative network management and protection: *Actuality is more difficult to maintain a system secured from the different threats that exist on a network, this results in more complex security management for network managers. This paper briefly summarizes Security Information and Event Management systems (SIEM), it reviews the main characteristics and continues with a description of OSSIM Alienvault System, showing its components and architecture.*

Keywords: Management, Security, SIEM, OSSIM.

Introducción

Debido a que el número de amenazas aumenta día a día, garantizar la seguridad adecuada en una red se ha hecho cada vez más difícil. Si bien existen una enorme cantidad de programas y técnicas para poder gestionar la seguridad de red, poder administrarlos todos se vuelve una tarea muy complicada.

Actualmente, una buena manera de gestionar la contabilidad de información de seguridad es utilizando los sistemas SIEM. Los sistemas SIEM actúan como un repositorio central registrando eventos de seguridad generados en la red. Estos sistemas le permiten al administrador de red, por medio de reglas lógicas, escoger ciertos eventos específicos de interés [1], permitiéndole al administrador realizar diversas tareas de monitoreo, vigilancia y diagnóstico dentro de una única interfaz de trabajo. En este artículo se expone un sistema SIEM en particular (OSSIM de Alienvault) el cual se ha ubicado como uno de los mejores exponentes de estos sistemas, integrando diversas herramientas de código abierto, como Nagios, Snort, OSSEC, entre otras.

A continuación se realiza una breve descripción de los sistemas SIEM, exponiendo sus componentes y características principales, seguido de una breve descripción y modo de funcionamiento del sistema del OSSIM Alienvault.

¿QUÉ ES SIEM?

El acrónimo SIEM se atribuye a los analistas de Gartner Amrit Williams y Nicolett Marcos y se deriva de dos tecnologías independientes, pero complementarias: el Administrador de Eventos de Seguridad (SEM por sus siglas en inglés) y el Administrador de Información de Seguridad (SIM por sus siglas en inglés). Durante la última década, estas dos tecnologías han convergido en una única solución conjunta conocida hoy como SIEM. SEM fue una solución tecnológica que se centró en el seguimiento de eventos de seguridad en tiempo real, así como la correlación y el procesamiento. Estos eventos de seguridad eran típicamente alertas generadas por un dispositivo de seguridad de red, tales como un firewall o un Sistema de Detección de Intrusos (IDS por sus siglas en inglés). SIM, por otra parte, se centró en el análisis histórico de la información del archivo de registro para apoyar las investigaciones forenses y los informes. SIM a menudo analiza los mismos eventos que SEM, pero no lo hace en tiempo real. SIM centraliza el almacenamiento de registros y archivos, búsqueda y análisis de funciones y, sólidas capacidades de presentación de informes. Los sistemas SIEMs combinan las capacidades de cada una de estas tecnologías en una única solución, de hecho, las soluciones SIEM actuales con frecuencia incorporan una función de gestión de registros mucho más amplia [3].

ARQUITECTURA BÁSICA DE LOS SISTEMAS SIEM

Los sistemas SIEM pueden ser comparados con una máquina compleja que posee un gran número de partes donde cada una realiza un trabajo específico e independiente. Todas estas partes deben colocarse a trabajar juntas adecuadamente o de lo contrario el sistema caerá en caos [1]. La figura 1 muestra la arquitectura básica de este tipo de sistemas.

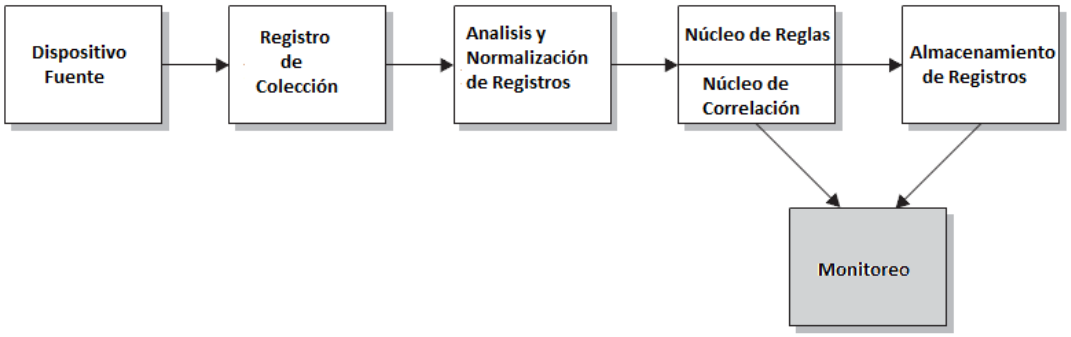

Figura 1. Arquitectura básica de un sistema SIEM [1].

A continuación se describen las partes o módulos que aparecen en la figura.

Dispositivo Fuente: La primera parte de un sistema SIEM es el dispositivo que captura la información. Un Dispositivo Fuente es el dispositivo, aplicación que recupera los registros que se almacenan y procesan en el SIEM. El dispositivo de origen puede ser un dispositivo físico en la red (como un router, un switch, o algún tipo de servidor), aunque también pueden ser los registros de una aplicación o cualquier otra información que puede adquirir1 como por ejemplo firewalls, servidores proxy, IDS, Sistemas de Prevención de Intrusiones (IPS por sus siglas en inglés), bases de datos, entre otros. Su comunicación con el resto del sistema puede ser mediante protocolos estándares o protocolos privativos, dependiendo del fabricante de sistema [1].

Registro de Colección: La siguiente parte del sistema es el dispositivo o la aplicación de flujo de registro, el cual obtiene de alguna manera todos los registros de los dispositivos fuentes para luego transportarlos al SIEM. Actualmente, la recolección de datos ocurre de diferentes maneras y a menudo depende del método implementado dentro del sistema final, pero en su forma más básica, los procesos de recopilación de registros se pueden dividir en dos métodos fundamentales de colección: o el Dispositivo Fuente envía sus registros al SIEM, lo que se llama el método de empuje, o el SIEM se extiende y recupera los registros del dispositivo de origen, lo cual se llama el método de extracción. Cada uno de estos métodos tiene sus aspectos positivos y negativos cuando se utilizan en un determinado entorno, pero ambos logran obtener los datos desde el dispositivo de origen en el SIEM [1, 3].

Análisis/Normalización de Registros: En este punto, los registros están todavía en su formato original en el repositorio centralizado y por tanto no resultan muy útiles para el sistema. Para que estos registros resulten útiles para el SIEM se les debe dar un formato estándar, lo cual se conoce como normalización. La normalización de los eventos no sólo hace que sean fácil de leer estos registros, sino que también facilita y permite un formato estándar para la generación de reglas del sistema, lo que significa que cada SIEM se encarga de las reglas de normalización de diferentes maneras. El resultado final es que todos los registros poseen el mismo aspecto dentro del sistema. Con frecuencia, antes de la normalización de los datos, se realizan copias de los registros, las cuales se almacenan en su formato original dentro del Log Storage [1, 3].

Núcleo de Reglas/Núcleo de Correlación: Este componente se encuentra dividido en 2 segmentos, el Núcleo de Reglas y el Núcleo de Correlación de Reglas. El Núcleo de Reglas amplía la normalización de los eventos con el fin de activar alertas en el SIEM debido a las condiciones específicas en estos registros. Estas reglas generalmente vienen predefinidas en el sistema, pero también se pueden definir reglas personalizadas. Por lo general, se pueden escribir estas reglas usando una forma de lógica booleana para determinar si se cumplen condiciones específicas y analizar patrones en los campos de datos [1], pero se debe tener precaución para evitar el establecimiento de reglas de correlación demasiado complejas o demasiadas reglas, ya que cada nueva norma aumentará exponencialmente los requisitos computacionales y, eventualmente, pueden hacer que el proceso de correlación resulte ineficaz [3]. La función del Núcleo de Correlación es comparar todos los eventos normalizados de diferentes fuentes con las reglas anteriormente creadas.

Almacenamiento de Registros: Este es usado para facilitar el trabajo en un único almacén de datos, facilitando la relación entre las diferentes funciones del SEM y las funciones forenses e informes del SIM. Su acoplamiento puede parecer sencillo, pero puede presentar una serie de retos y consideraciones. Este puede ser una base de datos, un archivo de texto plano o un archivo binario [1], ubicado de forma central o distribuida en dependencia al tamaño de la empresa, la cantidad de datos que son recogidos, y la infraestructura de TIC (Tecnologías de Información de Comunicación) [3].

Monitoreo: Una vez que el SIEM tenga todos los registros y los acontecimientos que se han procesado, se necesita hacer algo útil con la información. Un SIEM tendrá una interfaz de consola y una interfaz que bien puede ser o basarse en una aplicación web. Ambas interfaces le permiten visualizar y analizar todos los datos almacenados en el SIEM, facilitando de esta manera la gestión del sistema, pues brinda a los administradores una única visión de todo el entorno. También aquí se puede desarrollar el contenido y las reglas que se utilizan para extraer la información de los eventos que se están procesando [1].

OSSIM

OSSIM Alienvault (Open Source Security Information Manager) es un SIEM desarrollado por Dominique Karg y Julio Casal en el año 2000, que implementa la detección y prevención de intrusiones, y la seguridad de redes en general. Este sistema funciona a partir de múltiples herramientas populares de monitoreo y seguridad de código abierto (Open Source), como Nagios, Snort, y otros, gracias a lo cual ofrece grandes capacidades y un alto rendimiento, creando así una inteligencia que traduce, analiza y organiza los datos de una forma única que la mayoría de sistemas SIEM no pueden conseguir, resultando en un diseño que gestiona, organiza y observa riesgos que los administradores pueden apreciar [5]. Esta razón los ha convertido en la primera empresa de seguridad gratuita para grandes compañías y sistemas en el mundo, de la que actualmente se descargan 40.000 copias al año, (lo que representa el 50% de los despliegues de sistemas de seguridad del mundo), compitiendo con las grandes compañías de su negocio como IBM o McAfee [4].

Las principales características del OSSIM son [6]:

Realiza detección a bajo nivel y en tiempo real de la actividad anómala:

- Análisis de comportamiento de red
- Gestión de registros forenses

- Realiza análisis del riesgo de seguridad
- Presenta informes ejecutivos y técnicos
- Arquitectura escalable de alto rendimiento
- Es gratuito

AQUITECTURA DE OSSIM

La arquitectura que maneja OSSIM es muy parecida a la arquitectura de un SIEM descrita anteriormente. OSSIM utiliza 3 elementos básicos y un elemento adicional disponible únicamente para la versión comercial de OSSIM, llamada Alievault Profesional SIEM [6]. Todos estos componentes son descritos a continuación y se observan en la figura 2:

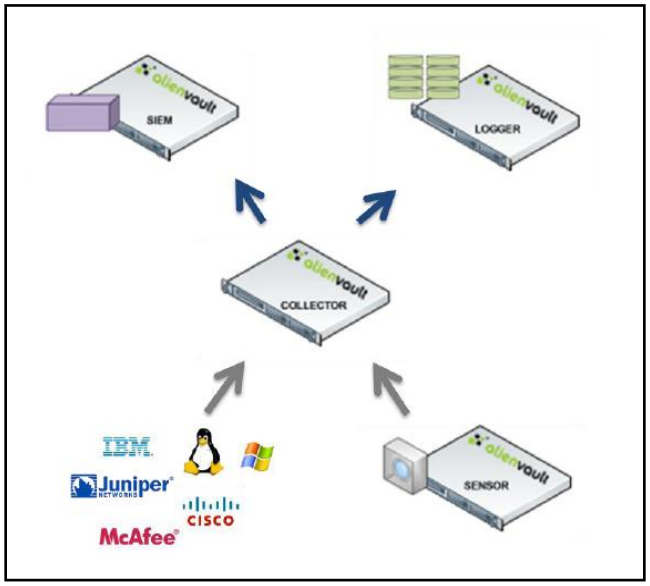

Figura 2: Arquitectura de OSSIM [6].

Sensores: son los encargados de recoger una amplia gama de información sobre su entorno local, procesar esta información y coordinar la detección y respuesta con el resto de la red OSSIM. Los sensores están instalados en los segmentos de red y lugares remotos, inspeccionan todo el tráfico, detectan ataques a través de diversos métodos y recolectan información sobre el tipo y forma de ataque sin afectar al rendimiento de la red [6].

Colectores: Los colectores reúnen los eventos generados por los sensores de OSSIM y cualquier otro sistema externo. Estos colectores clasifican y normalizan los acontecimientos antes de enviarlos al SIEM y al Logger. Con el objetivo de soportar el mayor número posible de aplicaciones y dispositivos, los colectores utilizan los Plugins Collection. Cada conector define cómo se recogen y se normalizan los eventos generados por cada dispositivo. Estos se pueden configurar mediante un archivo de configuración simple, utilizando expresiones regulares para definir el formato de cada tipo de evento. Los colectores pueden ser implementados como un sistema autónomo o ser incluidos en el sensor o dispositivo SIEM, en función de la necesidad de desempeño requerido [6].

SIEM: El SIEM proporciona inteligencia y capacidades de minería de datos al sistema de seguridad, que incluye evaluación de riesgos, correlación, indicadores de riesgo, análisis de vulnerabilidad y control en tiempo real. Aquí es donde se encuentran los núcleos de reglas y de correlación que proveen la inteligencia al sistema. El SIEM también incluye una base de datos SQL (Structured Query Language) que almacena la información normalizada, lo que permite un análisis profundo de la información y capacidades de minería de datos. El SIEM está diseñado para brindar un alto rendimiento y escalabilidad hasta muchos millones de eventos por día [6].

Logger : El Logger almacena eventos en formato "crudo" (sin modificar) en un dispositivo de seguridad forense. Los eventos son almacenados en masa y están firmados digitalmente, asegurando su admisibilidad como prueba en un "tribunal de justicia". El Logger permite el almacenamiento de un número ilimitado de eventos con fines forenses y se incluye únicamente para la versión pagada del OSSIM [6].

COMPONENTES DE OSSIM

Dentro de OSSIM Alienvault existe una gran variedad de las mejores herramientas Open Source, algunas de las más destacadas se enumeran a continuación [1]:

Snort: es el más importante IDS Open Source disponible en la actualidad. OSSIM contiene una versión personalizada de esta herramienta y es quien alerta sobre intentos de ataques a la red [1].

OpenVAS: es la versión GPL (General Public License) de Nessus, una popular herramienta de escaneo de vulnerabilidades Open Source. Esta herramienta se utiliza para proporcionar búsqueda de vulnerabilidades de los recursos de red y añade esta valiosa información a la base de datos de OSSIM. Nessus también es incluido dentro de OSSIM y es soportado utilizando un plug-in [7].

Ntop: es una popular herramienta Open Source para la monitorización del tráfico de la red. Esta herramienta proporciona información muy valiosa sobre el tráfico en la red, que puede ser utilizada para detectar de una manera proactiva el tráfico anormal o malicioso [7].

Nagios: es una popular herramienta Open Source de monitoreo de dispositivos de red. Es una de las herramientas más complejas, pero le permite al administrador tener una única visión del estado de los hosts de la red. A través del monitoreo de hosts, Nagios puede enviar alertas en caso de fallas y posee una interface web desde donde se puede observar el estado de la red [7].

PADS: El Sistema de Detección Pasiva de Activos (PADS por sus siglas en inglés) es una herramienta única. La herramienta supervisa silenciosamente el tráfico de red, los registros de los host y las actividades de servicio, con el objetivo de detectar anomalías sin generar tráfico de red, realizando un inventario de activos y revisando los servicios que cada cual ejecuta [7].

P0f: La herramienta P0f toma pasivamente las huellas dactilares del sistema operativo (el descubrimiento del tipo de sistema operativo y su versión). Esta herramienta escucha silenciosamente el tráfico de red e identifica los sistemas operativos que se comunican en la red. Esta información resulta útil en el proceso de correlación [7].

OCS-NG: La OCS-NG (Open Computer and Software Inventory Next Generation) ofrece la capacidad multi-plataforma de gestión de recursos. Esta herramienta permite mantener un inventario actualizado en tiempo real de los dispositivos existentes en la red [7].

OSSEC: Sistema de Detección de Intrusiones de Host (HIDS por sus siglas en inglés) Open Source. Este se encarga de analizar los datos del host y detectar a través de ellos si un host está siendo víctima de algún ataque.7 OSSEC realiza esta tarea analizando logs, chequeando la integridad de archivos, monitoreando el registro de Windows, detectando rootkits, además de responder y alertar en tiempo real. Esta herramienta también ayuda a proteger al propio OSSIM [7].

OSVDB: La OSVDB (Open Source Vulnerability Database), es la base de datos que mantiene la información actualizada con respecto a las vulnerabilidades del sistema. Esta se ha utilizado por OSSIM durante el proceso de correlación y es quien proporciona un análisis cuando sea necesario [7].

NFSen/NFDump: Visor de flujos de red para la detección de anomalías en la red. Este además permite el procesamiento de Netflow v5, v7 y v9. NFSen proporciona una interfaz gráfica basada en web a NFDump. Ambos NFSen y NFDump se han integrado en OSSIM y han sido modificados para trabajar con las otras herramientas [7].

Inprotect: Interfaz basada en web para Nessus, OpenVAS y NMAP. Inprotect ofrece la posibilidad de definir perfiles de escaneo, programar sondeos, y exportar los resultados del análisis de distintos formatos [7].

OSSIM también tiene otras destacadas herramientas como Arpwatch, el cual es utilizado para detección de anomalías en el uso de direcciones MAC, MACSpade, el cual es un motor de detección de anomalías en paquetes utilizados para obtener conocimiento de ataques sin firma, Tcptrack, que es utilizado para conocer la información de las sesiones, con lo cual puede conceder información útil relativa a los ataques, Osiris, que es un HIDS, y Snare, quien colecciona los logs de sistemas Windows [8].

EXPERIENCIAS COMERCIALES

En la actualidad existen diversos entornos de red que requieren una gestión de seguridad más compleja que la gran mayoría de redes. Una de las características principales de OSSIM es su gran versatilidad gestionando la seguridad lo cual constituye la razón principal por la que grandes empresas utilizan la versión pagada de OSSIM. Experiencias como el metro de Madrid, es una de estas. Aquí OSSIM es el encargado de gestionar las redes Wifi con las que trabajan en el Metro, los sistemas de radiotelefonía, que son con los que se realiza la comunicación con los trenes, los sistemas de explotación responsables del funcionamiento de los trenes por las vías, las cámaras de vídeo, torniquetes, expendedoras de billetes, carteles de información sobre trenes, entre otros [4]. Otra de sus aplicaciones se encuentra en el campo de la automática, y es la manipulación de los sistemas de Supervisión de Adquisición de Datos y Control de Automatización (SCADA por sus siglas en inglés) los cuales le permiten a los operadores controlar, monitorear y automatizar las actividades de los medios físicos conectados a estos sistemas, como combustibles, válvulas de gasoductos, sistemas refrigerantes, entre otros [9]. OSSIM también se ha extendido sobre entornos empresariales, la NASA (National Aeronautics and Space Administration), Telefónica España y la armada norteamericana, en donde ha demostrado excelentes resultados [9, 10].

En la actualidad, OSSIM posee un grupo de desarrolladores de entre 30 y 40 personas a nivel mundial de universidades como la de Pequín y grandes empresas, como Philips, además de tener una gran acogida a nivel mundial, con empresas socias en la India, Sudáfrica, Singapur, Nueva Jersey, Colombia, entre otros [4-11].

CONCLUSIONES

La seguridad de una red siempre ha sido y será un aspecto importante a considerar en cualquier entorno. Si bien en la actualidad existe una amplia gama de herramientas encargadas de gestionar la seguridad, es muy difícil para un administrador integrar su operación y funcionamiento. Los sistemas SIEM demuestran ser una buena alternativa de gestionar la seguridad de red, utilizando una interfaz común. Hay que tener en cuenta que a pesar de que los SIEM's hacen la vida más fácil a los administradores de red, no resuelven todos los problemas de seguridad. Los administradores deben de tener en cuenta el entorno donde se encuentran y conocer muy bien sus vulnerabilidades para que el sistema SIEM funcione correctamente.

OSSIM por su parte, es un SIEM Open Source, lo cual le da ciertas ventajas sobre muchos otros SIEM propietarios como:

Es gratis.

- Es compatible con la mayoría de los dispositivos actuales.

- Mantiene actualizado el sistema, sin costo alguno o reinstalación completa, pues detrás de cada herramienta Open Source contenida en OSSIM, existe una amplia comunidad que mejora el rendimiento de estas de manera gratuita.

- Es adaptable al entorno donde opere, pudiendo ser utilizado en redes sobre varios campos de la industria, como lo ha demostrado con sus aplicaciones en sistemas SCADA, entornos empresariales y sistemas de transporte, entre otras.

REFERENCIAS

1. R. MILLER, DAVID. HARRIS SHON, A. HARPER, ALLEN. VANDYKE, STEPHEN. BLASK, CHRIS: Security Information and Event Management (SIEM) Implementation. Ed. McGRAW HILL. New York, USA. 2011. Páginas 54-91. Libro Digitalizado

2. R. MILLER, DAVID. HARRIS SHON, A. HARPER, ALLEN. VANDYKE, STEPHEN. BLASK, CHRIS: Security Information and Event Management (SIEM) Implementation. Ed. McGRAW HILL. New York, USA. 2011. Páginas 140-142. Libro Digitalizado

3. SIN AUTOR: "Security Information and Event Management: Business Benefits and Security, Governance and Assurance Perspectives": ISACA: 2010. Páginas 5-6. Articulo Digitalizado.

4.RUIZ DEL ÁRBOL, MARUXA: "Regala tu producto y vencerás". 2010. disponible en: http://www.cincodias.com/articulo/empresas/regala-producto-venceras/20100812cdscdiemp_22/

5. BOWLING, JERAMIAH: "AlienVault: the Future of Security Information Management". 2010. disponible en: http://www.linuxjournal.com/magazine/alienvault-future-security-information-management?page=0,0

6. LORENZO, JUAN MANUEL: "Alievault Users Manual", Manual de ayuda de OSSIM.

7. SIN AUTOR: "Monitoreo de Red", Articulo digitalizado disponible en: http://www.qualydat.com/en/exito/46-casos-de-exito/114-monitoreored.html

8. SIN AUTOR: "OSSIM", Articulo digitalizado disponible en: http://es.wikipedia.org/wiki/Ossim

9. P. MELLO, JOHN: "New security appliance for SCADA systems introduced". 2011. Articulo digitalizado disponible en: http://www.gsnmagazine.com/node/23449

10. ROITER, NEIL.: "AlienVault Unified SIEM Bundles Security Tools For MSPs And Enterprises". 2011. Articulo digitalizado disponible en: http://www.networkcomputing.com/wan-security/229500332?pgno=1

11. MOLIST, MERCÈ: "una 'suite' libre de seguridad hecha por españoles triunfa en medio mundo", 2008. Disponible en: http://www.laneros.com/archive/index.php/t-131111.html