Implantación De Una Herramienta Ossim Para El Monitoreo Y Gestión De La Seguridad De La Red Y Plataformas Windows Y Linux Aplicado A Empresas Medianas

Ángel Heraldo Bravo Bravo[1]
Álvaro Luis Villafuerte Quiroz[2]
Ing. José Patiño S.[3]
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
[1]email: ahbravo@espol.edu.ec
[2]email: alvillaf@espol.edu.ec
[3]email: jpatino@espol.edu.ec

[1]Licenciado en Redes y Sistemas Operativos
[2]Licenciado en Redes y Sistemas Operativos
[3]Director Del Proyecto de Graduación, Máster en Sistemas, Ing. en Telecomunicaciones, ESPOL

Resumen

El presente artículo consiste en presentar un análisis de la seguridad de la infraestructura de red y de los servidores en una empresa privada, el enfoque principal es de mantener centralizado todos los eventos "logs" que son generados por los diferentes servidores y equipos de red en una sola consola de administración y realizar un análisis detallado de cada evento, así mismo como obtener reportes personalizados de las vulnerabilidades existentes en los hosts que corren bajo el sistema operativo Windows, de ataques ocasionados y del estado de la red en general .

Es así que por medio del desarrollo de este documento se busca presentar una solución informática con la implementación de la herramienta llamada OSSIM, siendo una aplicación Open Source y más que una herramienta de monitoreo de eventos "logs" también es un SIEM (Security Information and Event Management) y trae incorporado diversas formas para gestionar la seguridad en la red, bases de datos, analizar virus y malwares en plataformas Windows, OSSIM específicamente está orientado a los Administradores de red de empresas medianas que necesitan tener un monitoreo general de su infraestructura, obtener reportes en tiempo real de lo que está sucediendo en la red para poder analizar las anomalías y le ayuden en la toma de decisiones y correcciones oportunas.

Palabras Claves: *OSSIM Rsyslog, Componentes de Ossim, escaneo de Vulnerabilidades, Disponibilidad de la red.*

Abstract

This article is to present an analysis of the security of the network infrastructure and servers in a private company, the main focus is to keep centralized all events "logs" that are generated by different servers and network devices a single management console and perform an analysis of each event, also getting custom reports of vulnerabilities on hosts that run under the Windows operating system, the different attacks in the devices and the status of the network in general.

Thus, through the development of this document, we are to present a software solution with the implementation of the tool called OSSIM, this software is an open source application and It isn't a just a tool to monitor events "logs" it's also a SIEM (Security Information and Event Management) and has a built tools and more ways to manage network security, databases, analyze viruses and malware on Windows systems operating, OSSIM is specifically aimed for network manager of the medium companies that need a comprehensive monitoring infrastructure, get real-time reports of what is happening in the network to analyze anomalies and to help in making decisions and corrections.

Keywords: OSSIM Syslog, Ossim Components, vulnerability scanning, network availability.

1. Introducción

Las estadísticas mundiales presentan que el uso del internet tiene un crecimiento exponencial, los proveedores de servicios de internet en sus informes de ventas establecen un crecimiento en la demanda de los usuarios, esto se origina por la facilidad que tienen los usuarios de adquirir equipos Smartphones, los mismos que permiten la navegación a muchos servicios en la internet. Entonces la pregunta es ¿En que afecta el crecimiento del internet a las empresas?, Las empresas cambian su mercado acorde a la tecnología y aprovechando el mercado digital se ven en la obligación de llegar a los usuarios con diferentes servicios, y para esto hacen el uso de redes convergentes y servidores que puedan soportar el tráfico interno y externo.

Las empresas medianas en la actualidad invierten en redes de datos y voz, esta red esta apta para soportar todo el tráfico requerido por los usuarios y permite compartir diferentes recursos, adquieren servidores robustos con sistemas operativos multiplataforma capaces de brindar varios servicios a los usuarios internos y externos, y obviamente que con mayor cantidad de servicios y equipos accediendo a la red, también crece la complejidad de la administración, sin embargo intrusos, los hackers y delincuentes informáticos cada vez encuentran nuevas formas para continuar con su accionar y esta situación ha llevado a la aparición de nuevas amenazas que desean ingresar en los sistemas computarizados.

En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles, la posibilidad de interconectarse a través de redes han abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Es en este sentido, la importancia de tener una herramienta para visualizar en tiempo real el funcionamiento de la red y verificar los sucesos que están siendo ocasionados por los usuarios o atacantes a nuestra red y servidores.

La Seguridad Informática necesita de una herramienta que le ayude al administrador de la red a la toma de decisiones oportunas en la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

2. Marco Teórico

2.1 OSSIM

La sigla OSSIM se deriva para Open Source Security Information Management (Herramienta de Código Abierto para la Gestión de Seguridad de la información), OSSIM no es una herramienta única, al decir OSSIM se entiende que es un conjunto de herramientas unidas en un solo programa que facilita el análisis, visualización y la gestión de manera centralizada de los eventos que ocurren en los diferentes componentes de la infraestructura IT de la empresa, obteniendo de esta forma mayor efectividad a la hora del monitoreo y de encontrar errores u vulnerabilidades en la seguridad de la red.

OSSIM es una herramienta que nos ayuda mucho en el monitoreo de la red, permitiéndonos controlar algo tan básico desde un log de la contraseña mal digitada hasta un posible ataque que se esté dando a nuestra infraestructura.

Esta herramienta trae incorporada cerca de 22 Funciones, todas estas son Open Source capaces de correlacionarse y así poder tener el control centralizado, básicamente se lo puede representar en el siguiente diagrama.

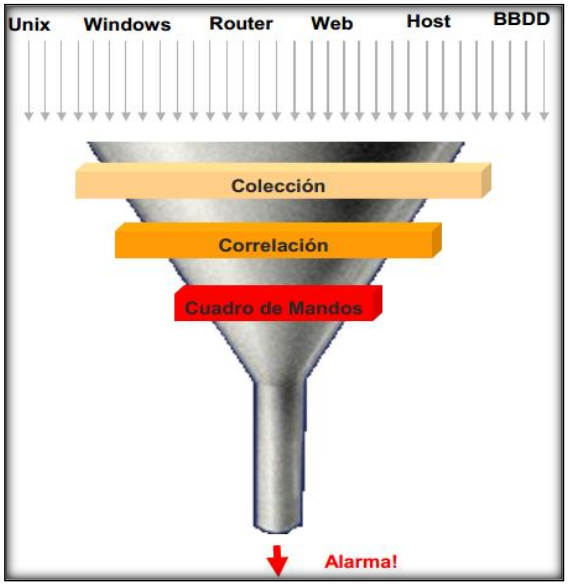

Figura 1: Modelo de OSSIM

2.2 Características de OSSIM

Ossim trae un conjunto de características que permite al administrador de red gestionar de forma más eficiente la seguridad interna de los servidores,

de la red de datos y voz, entre las cuales podemos mencionar los siguientes:

- Es gratuito.
- Monitoreo centralizado.
- Analiza el comportamiento de nuestra Red
- Presenta informes técnicos.
- Realiza un análisis de los posibles riesgos y anomalías en la red.
- Controla los posibles ataques/intruso en la red.
- Monitorea el excesivo tráfico que se pueda generar.
- Presenta una interfaz gráfica web amigable hacia al Administrador
- Permite recolectar logs de los servidores sin importar que distribución de Linux tenga instalado.
- El cliente recolector de logs que se instala en Windows es muy sencillo de configurar.
- Realiza test de vulnerabilidad.
- Realiza notificaciones automáticas mediantes alertas.

2.3 Componentes y Arquitectura

OSSIM tiene una arquitectura abierta, siendo OsssimServer el eje central de esta arquitectura, compartiendo con el Ossim-Framework y el Ossim-Agent.

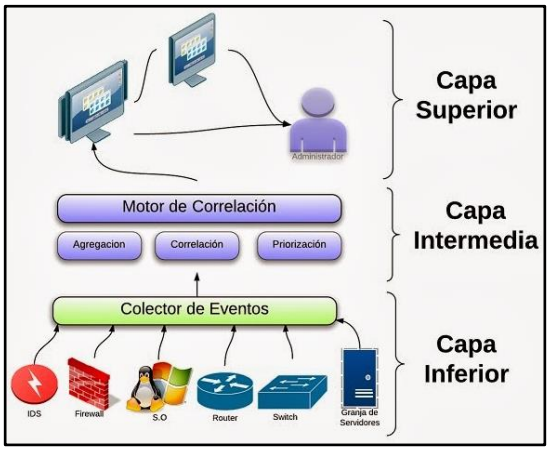

Figura 2: Arquitectura de OSSIM

Ossim-server: Como toda aplicación, Ossim funciona con un estándar cliente servidor y es obligatorio tener un solo servidor en toda nuestra red en el cual al instalar el perfil server (servidor) estamos configurando el ambiente que se encargue de procesar y recoger todos los logs que son generados por los diferentes dispositivos y servidores de nuestra red interna.

Ossim-framework: Esta componente sirve como intermediario para que la aplicación web del servidor no haga tareas en segundo plano como la lectura y escritura de la información que recibe, evitando así un innecesario uso de requerimiento como memoria y almacenaje y optimizar su funcionabilidad. Podemos mencionar que los propósitos primordiales de este componente son:

- Recolectar datos de los agentes y otros servidores
- Priorizar los eventos recibidos.
- Correlacionar los eventos recibidos de diferentes fuentes
- Realizar la evaluación de riesgos y disparar alarmas
- Almacenar eventos en la base de datos
- Reenviar eventos o alarmas a otros servidores

Ossim-agent: El nombre de Agent en la herramienta Ossim se les da a los plugins y aplicaciones que permite analizar todos los eventos específicos que se generan en la red de trabajo o en los diferentes servidores en la cual se está haciendo el monitoreo y seguimiento.

2.4 Escaneo de Vulnerabilidades

Osssim más que una herramienta de monitoreo de eventos “logs”, también es un SIEM (Security Information and Event Management) y trae incorporado diversas formas para gestionar la seguridad tales como:

- Antivirus que se encarga de detectar y eliminar software malicioso de los sistemas informáticos Windows, cuenta con
- Detectores de intrusos basados en host (HIDS, Host-based Intrusion Detection Systems) encargado de monitorear procesos y archivos críticos del sistema bajo análisis, cuenta con
- Detectores de intrusos basados en red (NIDS, Network-based Intrusion Detection Systems) responsables de la revisión de los datos que circulan por la red y avisan cuando observan tráfico que evidencia un ataque,
- Detectores de vulnerabilidades (Snort) que hacen un análisis detallado y arrojan como resultado las vulnerabilidades que existen en el sistema operativo y el software instalado,
- Detectores de disponibilidad que permiten verificar si el estado del equipo a monitorear se encuentra UP(activo) o DOWN(caído).

3. Fase de Implementación

Para poder realizar la implementación de OSSIM es necesario tomar en cuentas los siguientes factores:

3.1 Requisitos técnicos

El requisito técnico más importantes es el hardware para instalar OSSIM AlienVault, este dependerá en gran medida del número de eventos que tenga que procesar el servidor, de la cantidad de datos que pretendamos almacenar en la base de datos de OSSIM, y de la cantidad de hosts disponibles en la red que pretendamos analizar:

3.2 Requisitos del personal

Es muy importante que el administrador cumpla con los siguientes conocimientos mínimos:

- Debe tener conocimientos fundamentales de seguridades informáticas.
- Debe tener conocimientos básicos en Sistemas operativos Linux.
- Debe tener conocimientos en Sistemas operativos Windows Server.
- Debe saber interpretan los logs generados por los diferentes eventos en los sistemas operativos.
- Debe Tener conocimientos básicos del modelo TCP/IP
- Debe tener conocimientos básicos de Redes LAN/WAN.
- Debe tener conocimientos de seguridades en redes de Datos.
- Debe saber interpretar gráficos estadísticos de reportes.

3.3 Parámetros de configuración

Es muy importante configurar los parámetros adecuados en el servidor OSSIM para poder recolectar los eventos de forma eficiente, los parámetros personalizados más importantes son:

- Configuración de los parámetros de red
- Configuración al panel de Administración vía Acceso Web
- Puerto por donde escucha el servidor

4. Análisis Final

Según el análisis que hemos obtenido después de la instalación de la herramienta, los podemos clasificar en:

4.1 Análisis de resultados

Los parámetros que analizamos son la forma de configurar Ossim, el funcionamiento con la activación de los diferentes plugins y los resultados proporcionados por los informes que genera Ossim en producción, dando como resultado el cumplimiento de los objetivos planteados inicialmente y el éxito de la instalación en el servidor podemos estipular que es muy sencilla.

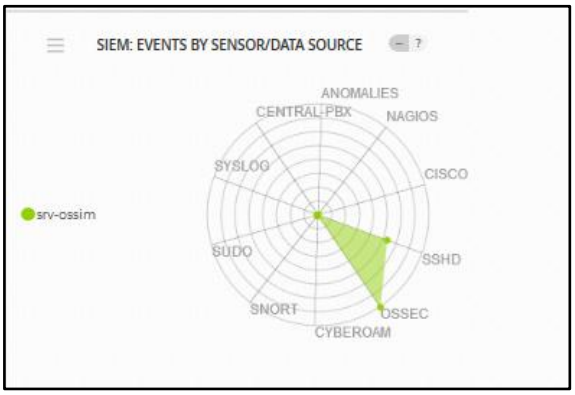

Figura 3: Análisis resumido de los Sensores

4.2 Análisis de Factibilidad.

La factibilidad de Ossim se destaca por tener una amplia gama de recursos que podemos utilizar y cubrir un mayor control en la seguridad, acorde a lo analizado en la instalación y funcionabilidad de la herramienta, podemos recalcar que es factible la instalación y puesta en marcha en cualquier empresa privada o pública dado que no representa una carga mayor al administrador de red y al ser una herramienta libre tampoco tiene una mayor carga económica para la empresa.

4.3 Análisis Financiero

El análisis financiero o la inversión que la empresa debe asumir están enfocados específicamente al Costo de implementación por parte del profesional en OSSIM y la adquisición de un servidor físico para su instalación. Para una mayor claridad, estos costos son reflejados en la siguiente tabla

COSTO DE IMPLEMENTACIÓN	
Licenciamiento	$ 0
Administrador de la red interna	IT
Servidor Fisico requerido.	$800
Consultor externo seguridad IT	$800
Ing Especialista en Ossim	$800
Movilización	$80
Alimentación	$150

Tabla 1: Costo Implementación del Proyecto

5. Conclusiones y Recomendaciones

1. Concluimos que en nuestro análisis destacamos que OSSIM no solo es una herramienta que recolecta logs de diferentes dispositivos, también es un SIEM (Security Information and Event Management) y trae incorporado diversas formas para gestión de seguridad.

2. Concluimos que OSSIM otorga un aporte invaluable al administrador de red, brindándole información útil para la toma de decisiones en el campo de la seguridad y que enfocados en la visión principal hemos logrado integrar varios dispositivos de red de diferentes marcas y diferentes servidores Windows y Linux en la misma consola, logrando obtener un resultado confiable en la solución implementada. OSSIM al tener la filosofía de código abierto y libre distribución, permite la implementación de una consola centralizada a un costo relativamente bajo.

3. Recomendamos a Ossim como una herramienta muy poderosa al momento de visualizar la disponibilidad de los servidores y dispositivos de red, porque es de gran ayuda y eficaz en el momento oportuno de riesgos y amenazas generados en la red interna por los diferentes hosts, al mismo tiempo presenta una gran cantidad de información que puede ser analizada detalladamente.

4. Se recomienda al administrador profundizar sus conocimientos en el campo de seguridades informáticas y administración de Linux para aprovechar al máximo el funcionamiento de OSSIM.

5. Se recomienda que Ossim sea implementado a partir de empresas medianas para optimizar su gestión y el control de una gran cantidad de hosts, previo a esto se recomienda tener una administración organizada de equipos de Red y Servidores tanto en Netbios y su direccionamiento lógico IP para poder tener establecidas los parámetros de cada usuario antes de Instalar la herramienta

6. Referencias

[1] «Alien Vault,» [En línea]. Available: https://www.alienvault.com/open-threat-exchange/projects. [Último acceso: 26 septiembre 2014].

[2] A. Ossim, «AlienVault OSSIM,» 15 Septiembre 2014. [En línea]. Available: https://www.alienvault.com/open-threat-exchange/projects. [Último acceso: 15 Septiembre 2014].

[3] W. BLOG, «Wolfant's BLOG,» 15 Octubre 2014. [En línea]. Available: http://wolfant.insuasti.ec/?p=29. [Último acceso: 15 Octubre 2014].

[4] A. Vault, «Wikipedia,» 2014. [En línea]. Available: http://es.wikipedia.org/wiki/Open_Source_Security_Information_Management. [Último acceso: 10 12 2014].

[5] L. Martinez, «SecurityByDefault.com,» 03 Mayo 2013. [En línea]. Available: http://www.securitybydefault.com/2013/05/mi-analisis-de-alienvaultossim-421.html. [Último acceso: Septiembre 2014].

[6] A. A. Parriza, «angelalonzo.ec,» [En línea]. Available: http://www.angelalonso.es/doc-presentaciones/ossim-hakin9.pdf.

[7] N. C. L. M. JOSE ALVAREZ OROZCO, «Blogdiario,» 12 08 2012. [En línea]. Available: http://networkadmin.blogspot.es/. [Último acceso: 18 08 2013].

[8] K. Makino, «kinomakino.blogspot,» 18 03 2014. [En línea]. Available: http://kinomakino.blogspot.com/2014/03/ossim-pentesting-continuo-como-si.html. [Último acceso: 17 12 2014].

[9] V3ktor, «itfreekzone.blogspot,» 15 06 2010. [En línea]. Available: http://itfreekzone.blogspot.com/2010/06/monitoreo-de-red-ossim-review-parte-i.html. [Último acceso: 07 11 2013].

[10] S. c. S.A, «sifra.net.mx,» 2009. [En línea]. Available: http://www.sifra.net.mx/metodolog%C3%ADa/ppdioo.aspx. [Último acceso: 05 12 2014].

[11] Admin, «todoit.com.ve,» 16 05 2011. [En línea]. Available: http://todoit.com.ve/blog/2011/sobre-metodologia-de-gestion-de-redes/.

[12] M. M. Tenorio, «hermeschavez.,» 14 08 2009. [En línea]. Available: http://hermeschavez.files.wordpress.com/2010/11/manual-super-de-ossim.pdf.

[13] Bumiga, «xmind,» 18 08 2010. [En línea]. Available: http://www.xmind.net/m/CseF/.

[14] Hector, «inforleon,» 14 09 2010. [En línea]. Available: http://inforleon.blogspot.com/2010/09/ossim.html. [Último acceso: 02 11 2014].

[15] C. E. B., «coberturadigital,» 16 05 2014. [En línea]. Available: http://www.coberturadigital.com/2014/05/16/internet-en-ecuador-el-acceso-paso-del-3-al-404-en-10-anos/#comments.

[16] «Bajolared,» 16 05 2014. [En línea]. Available: http://www.bajolared.com/wordpress/ossim-como-plataforma-de-monitorizacion-y-gestion-de-informacion-de-seguridad/. [Último acceso: 28 10 2014].

[17] D. R. M. S. H. A. A. H. S. VanDyke, Security Information And Event Management (Siem) Implementation, 2010 ed., New York: McGraw-Hill Education, 2010.

[18] SUPERTEL, «Aeprovi,» 08 10 2008. [En línea]. Available: http://www.aeprovi.org.ec/index.php?option=com_content&task=view&id=299&Itemid=34.