Artículo de Investigación

Análisis de los sistemas centralizados de seguridad informática a través de la herramienta Alienvault Ossim

Analysis of centralized computer security systems through the alienvault ossim tool

Ferruzola Gómez, Enrique Colon; Bermeo Almeida, Oscar Xavier; Arévalo Gamboa, Lissett Margarita

Enrique Colon Ferruzola Gómez
eferruzola@uagraria.edu.ec
Universidad Agraria del Ecuador, Ecuador
Oscar Xavier Bermeo Almeida
obermeo@uagraria.edu.ec
Universidad Agraria del Ecuador, Ecuador
Lissett Margarita Arévalo Gamboa
larevalog3@unemi.edu.ec
Universidad Estatal de Milagro, Ecuador

Ecuadorian Science Journal
GDEON, Ecuador
ISSN-e: 2602-8077
Periodicidad: Semestral
vol. 6, núm. 1, 2022
esj@gdeon.org

Recepción: 03 Octubre 2021
Aprobación: 20 Diciembre 2021

URL: http://portal.amelica.org/ameli/journal/606/6063067005/

DOI: https://doi.org/10.46480/esj.6.1.181

Como citar:: Ferruzola Gómez, E. C., Bermeo Almeida, O. X., & Arévalo Gamboa, L. M. (2022). Análisis de los sistemas centralizados de seguridad informática a través de la herramienta Alienvault Ossim. Ecuadorian Science Journal, 6(1), 23-31. https://doi.org/10.46480/esj.6.1.181

Resumen: Se hace un análisis sobre el uso y la efectividad de los sistemas centralizados en la seguridad informática con el objetivo de mostrar que con esta herramienta libre podemos hacer un monitoreo de amenazas, para el efecto se hizo un estudio general de la herramienta informática utilizada para proteger información denominada ALIENVAULT OSSIM, es de código abierto y está enfocada en evaluar las vulnerabilidades de los sistemas de información y detección de intrusos, analizando cada uno de estos eventos para poder ofrecer un informe detallado de todas las operaciones monitoreadas, como funciones de recopilación, normalización y correlación de eventos. Con la finalidad de proteger sus datos y equipos los usuarios utilizan SIEM (Información de seguridad y administración de eventos) en la seguridad de red para proteger los datos accesibles a través de la misma y que puedan ser objeto de modificación, robados o mal usados, como una solución y es implementado para la dirección de gestión de amenazas y respuestas a incidentes. Afortunadamente, hay una manera de hacer uso de la gestión de SIEM, mediante la implementación de AlienVault's OSSIM (Open Source SIEM).

Palabras clave: vulnerabilidades, amenazas informáticas, software libre, seguridad informática.

Abstract: An analysis is made on the use and effectiveness of centralized systems in computer security in order to show that with this free tool we can monitor threats, for this purpose a general study of the computer tool used to protect information called ALIENVAULT OSSIM, is open source and is focused on evaluating the vulnerabilities of information systems and intrusion detection, analyzing each of these events to be able to offer a detailed report of all monitored operations, such as collection functions, normalization and event correlation. In order to protect their data and equipment, users use SIEM (Security Information and Event Management) in network security to protect data accessible through it and that may be subject to modification, stolen or misused, as a solution and is implemented for threat management and incident response management. Fortunately, there is a way to make use of SIEM management, by implementing AlienVault's OSSIM (Open Source SIEM).

Keywords: vulnerabilities, computer threats, free software, computer security.

Introducción

Los sistemas centralizados de seguridad informática son un conjunto de elementos organizados que cumplen un objetivo esencial en el mundo de la interconexión de las redes, como la de preservar la información del usuario.

La facilidad de los sistemas centralizados es la obtención de información en distintos terminales y estos pueden estar a su vez en red, que es la forma más práctica y fácil de obtener datos actualizados. Cuando se realiza correctamente, la centralización no sólo puede simplificar las tareas administrativas, puede mejorar la seguridad, la gestión de datos y ahorrar dinero al usuario o propietario.

Por consiguiente, las amenazas existentes en un sistema centralizado al no ser detectadas a tiempo causarían daños severos que pueden influir el futuro de la entidad atacada, por tal motivo si no se cuenta con una herramienta tecnológica adecuada para la detección de vulnerabilidades un intruso podría vulnerar los datos de una red.

En razón a lo antes mencionado, se determina que una de las herramientas de detección de intrusos más utilizada por los administradores de redes de varias empresas es AlienVault OSSIM que se encuentra en el mercado SIEM desde el año 2003.

AlienVault ofrece herramientas que tienen diferentes funciones para analizar la red varias de estas tienen un costo para poderlas utilizar, pero tienen una opción de versión libre denominada OSSIM.

OSSIM puede ser utilizado por pequeñas organizaciones, pero es más eficaz cuando es utilizado por grandes organizaciones donde existen múltiples dispositivos de red, tales como cortafuegos, IDS/IPS, servidores web, antivirus, etcétera.

OSSIM está integrado con otras herramientas de seguridad de código abierto incluyendo a, Snort, Ntop, OpenVAS, Arpwatch, OSSEC, Osiris, Nagios, OCS, Kismet, entre otras.

Para una adecuada seguridad de la información de una empresa es recomendable la utilización de la herramienta Alienvault OSSIM, debido a que se enfoca en el análisis de la seguridad de la red, y la información de los sistemas centralizados que son emitidas por la red.

La facilidad de los sistemas centralizados es la obtención de información en distintos terminales y estos pueden estar a su vez en red, que es la forma más práctica y fácil de obtener datos actualizados. Cuando se realiza correctamente, la centralización no sólo puede simplificar las tareas administrativas, puede mejorar la seguridad, la gestión de datos y ahorrar dinero al usuario o propietario.

Por consiguiente, las amenazas existentes en un sistema centralizado al no ser detectadas a tiempo causarían daños severos que pueden influir el futuro de la entidad atacada, por tal motivo si no se cuenta con una herramienta tecnológica adecuada para la detección de vulnerabilidades un intruso podría vulnerar los datos de una red.

En razón a lo antes mencionado, se determina que una de las herramientas de detección de intrusos más utilizada por los administradores de redes de varias empresas es AlienVault OSSIM que se encuentra en el mercado SIEM desde el año 2003.

AlienVault ofrece herramientas que tienen diferentes funciones para analizar la red varias de estas tienen un costo para poderlas utilizar, pero tienen una opción de versión libre denominada OSSIM.

OSSIM puede ser utilizado por pequeñas organizaciones, pero es más eficaz cuando es utilizado por grandes organizaciones donde existen múltiples dispositivos de red, tales como cortafuegos, IDS/IPS, servidores web, antivirus, etcétera.

OSSIM está integrado con otras herramientas de seguridad de código abierto incluyendo a, Snort, Ntop, OpenVAS, Arpwatch, OSSEC, Osiris, Nagios, OCS, Kismet, entre otras.

Para una adecuada seguridad de la información de una empresa es recomendable la utilización de la herramienta Alienvault OSSIM, debido a que se enfoca en el análisis de la seguridad de la red, y la información de los sistemas centralizados que son emitidas por la red.

Marco Contextual

Vulnerabilidades

Una vulnerabilidad en la tecnología de la información (TI), es un defecto en el código o diseño que crea un potencial punto de ataque de seguridad por un extremo o red.

Para López (2010) nos genera un concepto de vulnerabilidades:

Probabilidades que existen de una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos son vulnerables a la acción de los hackers, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo (p. 14).

Seguridad Informática

La definición de la seguridad informática se describe como un campo de la informática que se ocupa del control de los riesgos relacionados con el uso de la computadora.

De la misma manera, los medios tradicionalmente que tienen la finalidad de realizar este objetivo es intentar crear una plataforma de confianza y segura, diseñada para que los agentes (usuarios o programas) sólo puedan realizar acciones que se hayan permitido, esto implica especificar e implementar una política de seguridad que se centre en la protección de los datos confidenciales de la organización.

Para Urbina (2016) escritor del libro Introducción a la Seguridad Informática definió que:

La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta (p. 12).

Así mismo, la seguridad del equipo se puede definir como controles que se ponen en marcha para proporcionar confidencialidad, integridad y disponibilidad para todos los componentes de los sistemas informáticos. Estos componentes incluyen datos, software, hardware y firmware.

El tema está en cómo se implementan las estrategias de seguridad y es allí donde se presenta la brecha entre la percepción y la realidad" (Ramirez, 2015).

Para tener una adecuada seguridad en la empresa se debe tener en consideración los siguientes componentes:

El hardware es la parte física o tangible del equipo, como la tarjeta de memoria del sistema, la unidad de disco, etc.

El firmware es el software permanente que ejecuta los procesos de la computadora y es en su mayoría invisible al usuario, como las funciones de puesta en marcha que hacen que los elementos del hardware funcionen juntos.

El software es la programación que ofrece servicios al usuario y al administrador. El sistema operativo, el procesador de textos, los juegos de ordenador y el navegador de Internet son ejemplos de software que se encuentran comúnmente en un ordenador.

Según Ramirez (2015) Director de la seguridad de Cisco Latam explicó que:

La percepción que tienen los defensores de seguridad en las empresas es que sus procesos de seguridad están verdaderamente eficaces; la realidad es que su infraestructura de seguridad probablemente necesita mejoras (p. 2).

Según Galindo et al. (2016) de la Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica de la Universidad de San Carlos de Guatemala detalló que:

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro (p. 102).

Por tal motivo, las características más importantes de la seguridad de las redes que se debe tener en consideración según los siguientes autores es la tríada CID que se describen a continuación:

Efectividad.

Según Urbina (2016) expuso que dicho término:

Trata de lograr que la información sea la necesaria para desarrollar cualquiera de las tareas que se desarrollan en la empresa u organización y sea adecuada para realizar los procesos del negocio, proporcionándola de manera oportuna, correcta, consistente y accesible (p. 12).

Eficiencia.

"Significa que la información sea generada y procesada utilizando de manera óptima los recursos que tiene la empresa para este fin" (Urbina, 2016, p. 12).

Confidencialidad.

El Profesional en Ciberseguridad y Hacking Ético Néstor Muñoz afirmó que este término se determina como: "La propiedad de la información que busca asegurar que la misma es accedida únicamente por las personas autorizadas. La propiedad contraria a la confidencialidad se le conoce como Divulgación" (Perez & Muñoz, 2006).

Para complementar con el criterio de varios autores mencionados anteriormente se describe lo siguiente: Para la confidencialidad, tendrá que asegurarse de que la información esté disponible sólo para las personas autorizadas, debido a que dicha confidencialidad incluye la privacidad de la información que puede ser personal y sensible.

Proteger la integridad de los datos es también una preocupación primordial para la empresa que necesita la convicción de que la información no se vuelve inexacta, debido a los cambios no intencionados.

Finalmente, se trabajará con el administrador de TI para proteger la disponibilidad de los datos, o la capacidad de las personas permitidas para acceder al ordenador y su información cuando sea necesario.

La protección de estas cualidades es su principal objetivo como administrador de seguridad. Estas cualidades se llaman la tríada de la CID.

Hackers

Un hacker es una persona que utiliza un ordenador aplicando métodos alternativos de acceso a un sistema informático con el objetivo de lograr vulnerar las redes de comunicación sin tener algún acceso autorizado

Según Ellis & Brown (2018) argumentó que:

Muchos usuarios nos conectamos a redes wifis totalmente libres que son ofrecidas ampliamente por: universidades, aeropuertos, cafeterías, hoteles y otras empresas, pero en caso de que no estén familiarizado con ataques a diversos protocolos estos pueden producir cambios drásticos en la seguridad, esto garantiza al atacante vulnerar tu propia red y mantener fuera de servicio a cientos de ordenadores por mucho tiempo (p. 6).

Por esta razón, los hackers maliciosos pueden infiltrase y vulnerar los datos en cualquier red informática que deseen si no se tiene la seguridad de la red adecuada.

Para Lizama Mendoza (2015) autor del libro Hackers explicó que:

Las competencias informáticas de los hackers han evolucionado hasta una dimensión política con el llamado hacktivismo: un movimiento que promueve la defensa de internet como un medio privilegiado para la libertad de funciones.

En razón a lo antes mencionado, se debe tomar con responsabilidad e importancia el tema de la seguridad de la red en la organización, por tal motivo se deberá utilizar herramientas que cumplan con la función de

monitorear y analizar la red informática para que detecte las vulnerabilidades de los activos digitales a los que se conectan en dicha red.

Por tal motivo, en el presente artículo se mencionará como medida preventiva de seguridad la utilización del sistema de seguridad de la información AlientVault.

AlientVault OSSIM

Permite que los usuarios de esta herramienta permitan modificarlo, esto permite tener unos varios desarrolladores enfocados en su mejora, porque ellos piensan que todos deben tener acceso a una herramienta sofisticada de seguridad

Para Foster (2017) expone que una definición de la herramienta a utilizarse se encuentra en la página oficial:

OSSIM, seguridad de la información de código abierto de AlienVault y Gestión de Eventos de producto, le proporciona al usuario una fuente abierta de múltiples sistemas de recolección de datos que transitan por la red.

Para Perez & Muñoz (2006) afirmó en su libro que:

La característica principal de OSSIM es el procesamiento en paralelo, modelización rigurosa de sensores, asi como la característica de ser Open Source lo que facilita que se puede controlar en todo momento el procesado interno (P. 354).

Implementación de la herramienta ALIENVAULT OSSIM

Para el manejo óptimo de la herramienta se debe tener en cuenta los requisitos de software y hardware, el personal que maneje la herramienta debe tener varios conocimientos como seguridad informática y gráficos estadísticos, descubrimiento de activos, evaluación de vulnerabilidades, detección de Intrusos, supervisión y comportamiento del tráfico de la red.

TABLA 1
Herramientas que se incluyen en OSSIM

ACTIVA	PASIVA
Ocs: Gestión de Inventario.	Snort: Analiza todo el tráfico de red.
Nagios: Realiza comprobaciones en remoto.	Ntop: Ofrece datos en tiempo real e histórico.
OpenVas: Realiza escaneo de vulnerabilidades.	NFSen: Interfaz gráfica que permite gestionar y mostrar la información recogida.
OSSEC: Monitoriza el registro de Windows.	Nfdump: recoge y procesa netflows desde la línea de comandos.
Nmap: Escanea redes y equipos.	Kismet: Rastrea el tráfico.
	P0f: Detección de anomalías en sistema operativo.
	Pads: Detección de anomalías en servicios.
	Arpwatch: Detección de anomalías en las direcciones MAC.
	Tcptrack: Monitor de sesiones.
	Nepenthes: Emula servicios y vulnerabilidades conocidas con el objeto de recoger información.

Autores

Es un software de licencia libre (open source) que cumple con la funcionalidad de realizar el inventario de todos los activos dentro de la empresa.

"Ocs Inventory NG incluye la funcionalidad de implementación de paquetes para asegurarse de que todos los entornos de software que están en la red son los mismos" (Belliard, 2017).

Nagios es conocido por ser el mejor software de monitoreo de servidores en el mercado. La supervisión de servidores se hace fácil en Nagios debido a la flexibilidad para monitorear sus servidores con monitoreo basado en agentes y sin agente.

"Nagios contiene una monitorización completa de TI y software de alertas para servidores, redes y aplicaciones. Simplifica enormemente el proceso de búsqueda de sus datos de registros" (Nagios, 2017).

OpenVas es un marco de diversos servicios y herramientas que ofrecen una solución completa y potente de análisis de vulnerabilidades y gestión de vulnerabilidades.

El Sistema de Evaluación de la vulnerabilidad abierto (OpenVAS) es un marco de diversos servicios y herramientas que ofrecen una solución completa y potente de análisis de vulnerabilidades y gestión de vulnerabilidades.

"El escáner de seguridad real se acompaña con una fuente actualizada periódicamente de las Pruebas de vulnerabilidad de la red" (OpenVAS, 2016).

Nmap es un escáner de puertos, de redes y equipos que, mediante un escaneo configurable con precisión, velocidad, grado de intrusión.

Snort es un sistema de prevención de intrusiones de red de código abierto, capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes IP.

Además, puede realizar análisis de protocolo, búsqueda de contenido/coincidencia, y se puede utilizar para detectar una variedad de ataques y sondeos, tales como desbordamientos de búfer, escaneos de puertos furtivos, ataques cgi, sondeos SMB, intentos de huellas dactilares os, y mucho más.

"Snort es un software de detección, uno de los más potentes de código abierto, el cual es un sistema de instrucciones de tiempo real, analizando el tráfico de red y el registro de paquetes" (Snort, 2017).

"Ntop análisis basado en la web de alta velocidad de tráfico. Desarrolla software de red de alta calidad utilizado por los individuos pequeños, así por los grandes operadores de telecomunicaciones" (Franklin, 2018).

"Nfdump Es un conjunto de herramientas que lee los datos de NetFlow de los archivos almacenados por nfcapd, su sintaxis es similar a tcpdump" (sourceforge, 2017) .

NFSen ss una interfaz gráfica basada en web para los nfdump herramientas netflow. NFSen le permite:

- Visualizar sus datos netflow: Flujos, paquetes y bytes utilizando RRD (Round Robin base de datos).
- Fácil de navegar a través de los datos de NetFlow.
- Procesar los datos netflow dentro del período de tiempo especificado.
- Crear historia, así como perfiles continuos
- Establecer alertas, basado en diversas condiciones.
- Escribir sus propios plugins para procesar los datos netflow en un intervalo regular (sourceforge, 2017).

Ntop Es una red de herramientas de tráfico que muestra el uso de la red en tiempo real. Una de las cosas buenas de esta herramienta es que puede utilizar un navegador web para administrar y navegar a través de la información de tráfico Ntop para comprender mejor el estado de la red.

"Kismet es un detector de red, sniffer, y el sistema de detección de intrusiones inalámbricas. Kismet funciona predominantemente con Wi-Fi (IEEE 802.11) redes, pero se puede ampliar a través de plug-ins para manejar otros tipos de redes" (Bau, 2016).

Metodología

Diseño de investigación

Este trabajo de investigación surge del interés por adquirir un mejor sistema de seguridad informática, dado que no solo es importante tener sistemas informáticos en las empresas, sino mantener la información de éstos, segura, puesto que las redes de datos son activos importantes para las empresas, por lo que requieren ser protegidos frente a cualquier amenaza por medio de la red, que ponga en peligro la disponibilidad, integridad

y la confiabilidad de la información, la estabilidad de los procesos, los niveles de competitividad, la imagen corporativa, la rentabilidad y la legalidad, aspectos necesarios para alcanzar los objetivos de la organización.

Existen diversos problemas derivados de la presencia de vulnerabilidades en la red, lo que ocasiona pérdidas significativas para las empresas y usuarios en la actualidad, es por esto por lo que se ha desarrollado este estudio que permita la detección de dichas vulnerabilidades.

Como consecuencia de la utilización de esta metodología de investigación se ha explorado esta solución para la detección de vulnerabilidades en la red, de uso sencillo y soportado en una herramienta de código abierto, se presenta un enfoque práctico y conceptual para la detección y erradicación de vulnerabilidades que pueden ocasionar pérdida de información, ya sea por el ataque de hackers, personal que se van de la empresa y luego se lucran con la información, debido a la mala implementación de políticas y normas de seguridad; por lo tanto se debe de invertir en recursos de seguridad informática y resguardo de información.

Finalmente, como parte del diseño de la investigación se presenta un caso de estudio de aplicación de la herramienta propuesta, es así como se logra establecer la utilidad y funcionalidad de la misma.

Resultados y Discusión

Se ha encontrado que la correlación es una de las principales características que define OSSIM como una inteligente herramienta de gestión de eventos de seguridad de plataforma web y la distingue de IDS/IPS.

Además, ayuda a reducir el número de falsos positivos mediante la transformación de múltiples entradas de eventos y alarmas para una mayor fiabilidad del resultado, de modo que hay una cantidad manejable de eventos para prestar atención.

Una función de correlación consta de la correlación cruzada y correlación lógica (Correlación de directiva).

La correlación cruzada sólo funciona con eventos que han definido el destino IPs porque tiene que comprobar el host de destino para determinar si tiene cualquier vulnerabilidad.

El caso de la confiabilidad de valor es una de las métricas que se utiliza para calcular el riesgo en OSSIM.

Otra característica fundamental que se evidenció de OSSIM es la correlación de directivas.

OSSIM viene con 200 de ellas y están escritos en sintaxis basada en XML. La directiva tiene por objetivo principal analizar varios eventos y decidir si procede o no generar una alarma basada en directiva de reglas.

Esta función puede evitar los ataques de día cero (brecha en la seguridad) o vulnerabilidades desconocidas porque está generando una alarma por reglas siguientes, en contraposición a la comprobación del evento en la conocida lista de vulnerabilidades. Un ejemplo sencillo de la directiva podría ser para generar una alarma cuando alguien intenta conectarse con SSH (Secure Shell) en un servidor web varias veces.

OSSIM es altamente escalable y fácil de trabajar. Una cosa que se ha visto muy útil en lo que respecta a la característica de informes es su capacidad para crear un informe programado y por correo electrónico automáticamente.

Es bastante sencillo de instalar OSSIM, especialmente si se realiza la instalación por defecto automatizada, que se llama Perfil de all-in-one. Perfil de All-in-one incluye sensor, servidor, marco y base de datos de perfiles.

El perfil de sensor nos permitirá configurar el sistema para que podamos recibir registros de hosts remotos y dispositivos que utilizan el protocolo syslog.

Por defecto, muchas de las herramientas de código abierto conocido están habilitadas como detectores en Perfil de Sensor, como Snort, Ntop, OSSEC, Osiris, entre otras. Puede haber múltiples sensores en implantación de OSSIM si el número de redes que se monitorea es más de uno.

Así mismo, la responsabilidad de Perfil de servidor debe recibir registros normalizados del Sensor. OSSIM se gestiona a través de la interfaz de administración web, una vez que la instalación está completa, el perfil de marco es responsable de configurar el componente web GUI.

El perfil de base de datos utiliza como gestor de base de datos a MySQL para almacenar la información de configuración y eventos SIEM.

La primera cosa que se debe hacer durante la instalación de OSSIM es agregar sistemas de OSSIM supervisar y poner valores de los activos a los anfitriones.

La siguiente tarea fue conectar las fuentes de datos en el sensor para reenviar todos los registros en un lugar central para analizarlos.

La siguiente tarea importante es personalizar las directivas, las directivas de correlación y las reglas de modo que se reducen los falsos positivos y tienes la posibilidad de configurar casi cualquier tipo de condiciones para la activación de una alarma/ticket.

OSSIM proporciona la capacidad de procesar imágenes de cámaras satelitales y aéreas y transformarlas en mapas de imagen precisos asociados con posiciones tridimensionales en la tierra.

A menudo, estos instrumentos son capaces de capturar información espectral del espectro electromagnético fuera de nuestro rango visual. OSSIM permite que esta información sea procesada para una amplia variedad de aplicaciones, incluyendo la agricultura de precisión, la evaluación medioambiental y la planificación urbana.

Así mismo, al ser un software de código abierto es una opción atractiva para las organizaciones, estas versiones tienen numerosas cantidades de gente tratando de mejorar su código y ofrecer más facilidades, opciones que satisfaga un mercado que en la actualidad usa mucho este tipo de herramientas.

AlienVault OSIIM es una opción muy viable que, como departamento de seguridad, podrá mantener al tanto de personas no deseadas tengan acceso a información confidencial, y generar reportes oportunos para tomar las medidas pertinentes del caso.

Conclusiones

Se ha realizado el análisis sobre los procesos actuales que poseen las empresas, realizando pruebas en distintos escenarios de la red, con lo que se pudo identificar que las empresas actualmente no poseen procesos de monitorización para la seguridad de la red, lo cual es perjudicial en cierta medida ya que están expuestos a constantes problemas o amenazas que puedan suscitarse dentro de la misma.

La utilización de una herramienta que agrupa los datos de seguridad informática para la administración y monitoreo de la red en las empresas es de gran utilidad para los administradores de red y su mayor prioridad es que sea una herramienta de fácil manejo y comprensión, que les permita optimizar su gestión en cuanto a detección de anomalías y solución de los diferentes problemas que se les presente en la red, siendo una herramienta de código abierto y su costo es nulo; adquirirla e implementarla resultará de gran ayuda, ya que podrán reducir tiempo, personal y recursos que se utilizaban antes de implementarla.

Se puede concluir que OSSIM AlienVault es una herramienta que trabaja de manera inteligente permitiendo la correlación de eventos, detección de intrusos, monitoreo de los dispositivos que estén conectados a la red, y el envío de alarmas informando lo sucedido permite al administrador de red prevenir los incidentes y obtener los informes de lo sucedido en tiempo real para su corrección y seguridad de la red, de acuerdo con las encuestas se pudo verificar los objetivos.

Referencias Bibliográficas

Bau, S. (2016). *Kismet* . https://www.kismetwireless.net/

Belliard, D. (2017). *OCS Inventory NG*. https://ocsinventory-ng.org/?lang=fr

Ellis, S., & Brown, M. (2018). *El Método Hacking Growth*. Conecta.

Foster, G. (2017). *Alien Vault*. https://cybersecurity.att.com/products/ossim

Franklin, B. (2018). *ntop – High Performance Network Monitoring Solutions based on Open Source and Commodity Hardware*.https://www.ntop.org/

Galindo, C., Mena, A., Santizo, W., Mendoza, S., & García, M. (2016). *Seguridad de la Información*. Guatemala. Editorial Universidad de San Carlos de Guatemala

Lizama Mendoza, J. (2015). Hackers: de piratas a defensores del software libre. *Revista Mexicana de Ciencias Políticas y Sociales; Vol 45, No 185 (2002)*. http://www.revistas.unam.mx/index.php/rmcpys/article/view/48321

López, P. A. (2010). *Seguridad informática*. Editex.

Nagios. (2017). *Nagios* . https://www.nagios.org/

OpenVAS. (2016). *OpenVAS - Open Vulnerability Assessment Scanner*. https://www.openvas.org/

Perez, C., & Muñoz, A. L. (2006). *Teledetección: nociones y aplicaciones*. carlos perez.

Ramirez, F. (2015). *¿Podremos alcanzar la seguridad informática?* . https://www.estamosenlinea.com.ve/2015/04/01/podremos-alcanzar-la-seguridad-informatica/

Snort. (2017). *Snort - Network Intrusion Detection & Prevention System*. https://www.snort.org/

sourceforge. (2017). *sourceforge-NfSen*. http://nfsen.sourceforge.net/

Urbina, G. B. (2016). *Introducción a la seguridad informática*. Grupo editorial PATRIA.