ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

"IMPLEMENTACIÓN DE UN CORRELACIONADOR DE EVENTOS BASADO EN SOFTWARE LIBRE PARA LA DETECCIÓN DE ATAQUES INFORMÁTICOS EN LA EMPRESA ELÉCTRICA"

Trabajo de titulación

Tipo: Propuesta tecnológica

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

AUTORES: CRISTIAN ANDRÉS PAZMIÑO GÓMEZ

JORGE LUIS PAZMIÑO GÓMEZ

TUTOR: ING. ALBERTO LEOPOLDO ARELLANO AUCANCELA

Riobamba – Ecuador

2018

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

El Tribunal del Trabajo de Titulación certifica que: El trabajo de investigación: Tipo Propuesta Tecnológica **"IMPLEMENTACIÓN DE UN CORRELACIONADOR DE EVENTOS BASADO EN SOFTWARE LIBRE PARA LA DETECCIÓN DE ATAQUES INFORMÁTICOS EN LA EMPRESA ELÉCTRICA RIOBAMBA S.A"**, de responsabilidad de los señores Cristian Andrés Pazmiño Gómez y Jorge Luis Pazmiño Gómez, ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, quedando autorizada su presentación.

NOMBRE	**FIRMA**	**FECHA**
DR. JULIO SANTILLÁN **VICEDECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	_____	_____
ING. FRANKLIN MORENO **DIRECTOR DE LA ESCUELA DE INGENIERÍA ELECTRÓNICA, TELECOMUNICACIONES Y REDES**	_____	_____
ING. ALBERTO ARELLANO **DIRECTOR DEL TRABAJO DE TITULACIÓN**	_____	_____
ING. DIEGO VELOZ **MIEMBRO DEL TRIBUNAL**	_____	_____

Nosotros, Cristian Andrés Pazmiño Gómez y Jorge Luis Pazmiño Gómez, declaramos que el presente Trabajo de Titulación es de nuestra autoría y que los resultados del mismo son auténticos y originales. Los textos que constan en el documento y provienen de otra fuente están debidamente referenciados. Como autores, asumimos la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación.

Andrés, Jorge.

DEDICATORIA

Primero que todo quiero agradecer a Dios, por permitir llegar a esta instancia y por todos los factores que ello implique. Segundo quiero dedicar este trabajo a mis padres Alberto y Gloria por su amor y cariño, por ser los pilares fundamentales en mi vida, siendo el impulso para avanzar y por haber estado allí en todo momento. Con mucho énfasis quiero dedicar este trabajo a mi hermano Luis por todos los conocimientos impartidos y al ser una guía de manera profesional como personal, a mi hermano Jorge por ser mi compañero de Tesis y mi mejor amigo en la vida, a mi cuñada Naty por el apoyo y a mi sobrinita Nico, que con sus ocurrencias y su existir han alegrado mi vida. A mí enamorada Camila, por su comprensión y su apoyo en el desarrollo del presente, a mi Tutor Ing Alberto Arellano por sus conocimientos, a mis abuelitos en el cielo. Y dedicado con mucho amor a toda mi familia y amigos, por la constante motivación, su amistad y cariño.

Andrés

El presente trabajo se lo dedico a Dios que ha sabido guiarme y darme la fortaleza necesaria en todo este recorrido, a mis padres que me han apoyado en todo momento, siendo un pilar fundamental para mi crecimiento y formación en todos los aspectos de mi vida, a mis hermanos Andrés y Luis que nunca me dejaron desfallecer en todo este camino siendo mis mejores amigos desde que éramos niños. A mi sobrinita, que desde el día en que nació fue motivo suficiente para sonreír ante cualquier adversidad, a toda mi familia que con sus consejos siempre estuvieron poniendo su granito de arena para conseguir tan anhelada meta. Y por último a todas esas personas, que por razones de la vida ya no se encuentran presentes pero que, en su momento, con sus palabras y acciones fueron fundamentales para que este propósito se pueda realizar.

Jorge

AGRADECIMIENTO

En este presente trabajo de Titulación queremos agradecer a Dios por permitirnos llegar a esta instancia, al culminar una etapa académica más en nuestras vidas. A nuestros padres Alberto y Gloria por todo el amor, apoyo y esfuerzos realizados, al ser una guía para nosotros en todos los aspectos de la vida. A nuestro hermano Luis que ha sido un ejemplo a seguir y un pilar fundamental para nuestro crecimiento personal como profesional. A nuestro Tutor Ing. Alberto Arellano por sus conocimientos impartidos y en general a todos los docentes de la FIE-ESPOCH. Y por último a nuestra querida ESPOCH, que nos ha brindado experiencias inolvidables y la oportunidad de conocer grandes personas.

Jorge y Andrés

TABLA DE CONTENIDO

INDICE DE ABREVIATURAS

SIEM: Gestión de eventos e información de seguridad

DDoS: Distributed Denial of Service (Denegación de Servicio Distribuido)

DNS: Domain Name System (Sistema de Nombres de Dominio)

OSSTMM: Open Source Security Testing Methodology Manual (Manual de la Metodología Abierta de Testeo de Seguridad)

DoS: Denial of Service (Denegación de Servicio)

SQL: Structured Query Language (Lenguaje de Consulta Estructurada)

XSS: Cross Site Scripting

HTML: Hypertext Markup Language (Lenguaje de Marcas de Hipertexto)

TI: Tecnología de la Información

SEM: Security Event Management

SIM: Security Information Management

IDS: **I**ntrusion Detection System (Sistema de Detección de Intrusos)

IPS: Intrusion Prevention System (Sistema de Prevención de Intrusos)

OSSIM: Open Source Security Information Management (Gestión de Información de Seguridad de código abierto)

HIDS: Host-based Intrusion Detection System (Sistema de Detección de Intrusos en un Host)

NIDS: Network Intrusion Detection System (Sistema de detección de intrusos en una Red)

PCAP: Packet Capture

INDICE DE TABLAS

INDICE DE FÍGURAS

INDICE DE GRÁFICOS

RESÚMEN

El presente trabajo de titulación tuvo por objetivo la implementación de un correlacionador de eventos basado en software libre para la detección de ataques informáticos en la empresa eléctrica Riobamba S.A ya que, si bien poseen dispositivos de seguridad como el Firewall Check Point 4800, no cuentan con una solución centralizada que les permita recolectar, almacenar y gestionar logs provenientes de sus activos de información. Para dar solución a este problema se realizó un estudio comparativo entre varias plataformas y se determinó que la opción más adecuada es el sistema operativo "Security Onion" basado en Ubuntu, el cual se implementó sobre un servidor HP-Proliant con dos interfaces de red, la primera para la administración y la otra para la recolección del tráfico de red, para el envío de logs hacia el correlacionador de eventos, en los dispositivos de red se configuró SYSLOG y en los activos de red se instaló agentes OSSEC. La topología que utiliza el correlacionador de eventos es la de cliente-servidor. Los resultados tomados entre enero y febrero del 2018 fueron el total de ataques informáticos reportados por el correlacionador de eventos, mediante lo cual se pudo determinar que los principales ataques que se realizan son: denegación de servicio y ataques de fuerza bruta con un total de 2049 y 1910 incidencias respectivamente, siendo China la principal fuente de origen de los ataques con un total 1862. En base a los resultados obtenidos se pudo concluir que el correlacionador de eventos funciona de manera correcta, detectando ataques en tiempo real y a su vez generando las respectivas alertas; logrando así analizar el tráfico que circula por la red, se recomienda continuar con la investigación e incluir el procesamiento y estandarización de los logs de los sistemas "SCADA".

Palabras Clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>**,** <REDES DE COMPUTADORES>**,** <SEGURIDAD DE LA INFORMACIÓN>**,** <SEGURIDAD INFORMÁTICA>, <CORRELACIÓN DE EVENTOS>, <SOFTWARE LIBRE>, <SECURITY ONION (SOFTWARE)>.

SUMMARY

This work aimed at implementing a free software-based event correlator to detect cyber-attacks at the Riobamba S.A Electric Power Enterprise, since even though, it has security devices like Firewall Check Point 4800, it does not have a centralized solution collecting, storing, and managing the information asset logs. To solve this issue, a comparative study has been done among several platforms, so Ubuntu-based Security Onion is the most appropriate. It was implemented in a HP Proliant server with two interfaces: the first one is for managing and the other one is for gathering the network traffic. SYSLOG was set up in network device to send logs towards the event correlator, and OSSEC agents were installed in the network assets. There were 2018 cyber-attacks reported by the event correlator in the results from January and Frebruary. Therefore, it was possible to determine that the main attacks were: denial of service and brute force attack with a total of 2049 and 1910 incidences respectively. China was the main source of attacks with a total of 1862. Of the results, it is concluded that the event correlator detects attacks properly in real time and at the same time generates the respective alerts. As consequence, the traffic circulating in the network was analyzed. It is recommended to continue to investigate and include the log process and standardization of SCADA system.

Key words: <ENGINEERING SCIENCE AND TECHNOLOGY>, <COMPUTER NETWORK>, <INFORMATION SECURITY>, <EVENT CORRELATION>, <FREE SOFTWARE>, <SECURITY ONION (SOFTWARE)>

INTRODUCCIÓN

En la actualidad, la información es el bien más preciado para toda organización y en el intento por gestionar cualquier incidente de seguridad informática que pueda poner en riesgo la confidencialidad, integridad y disponibilidad de esta, han surgido dispositivos de seguridad perimetral, como son: IDS, IPS, Firewalls, y otros.

El problema radica, que, al momento de producirse un ataque informático, cada dispositivo de la infraestructura de red genera sus propios logs, dependiendo de su fabricante y el procesamiento de estos no es una tarea fácil ya que, los mismos poseen gran tamaño y son incompatibles entre sí, razón por la cual es necesario la normalización y centralización de estos, que nos permita de una manera más fácil generar alertas y detectar ataques informáticos en tiempo real.

En el presente documento se detalla la implementación de un correlacionador de eventos basado en software libre en la "Empresa Eléctrica Riobamba S.A", debido a la cantidad de ataques informáticos que se han venido suscitando.

Entre los principales ataques informáticos que se han realizado a dicha empresa se puede mencionar los siguientes: ataques de denegación de servicio a su página WEB, mail spoofing, cambios de contraseñas a las cuentas de correo electrónico.

Con el fin de probar la efectividad de esta tecnología, al final se detalla los resultados recopilados en el periodo de tiempo enero a febrero 2018, entre los cuales se muestran los ataques informáticos detectados, las fuentes de origen, los activos con mayores incidencias, entre otros.

Antecedentes

Con el fin de ofrecer un adecuado tratamiento a los activos de información han surgido diferentes técnicas con el objetivo de mitigar afectaciones a la confidencialidad, integridad y disponibilidad de la información, impidiendo que las amenazas se materialicen en incidentes y generen un riesgo, sin embargo, esta seguridad continúa siendo un reto para los atacantes informáticos, quienes utilizan métodos cada vez más complejos, con el fín de penetrar las redes de datos.(Heerden et al, 2013, pp. 1-7)

Como medida para contrarrestar estos ataques, se utiliza la práctica de los SIEM, que son la combinación de las tecnologías SIM y SEM, que constan con técnicas avanzadas para la correlación de eventos, dando a conocer de esta manera el estado de los sistemas corporativos en tiempo real a través del análisis de logs. (AlienVault Academy, 2014)

Hoy en día han surgido estudios sobre la tecnología SIEM, del cual se menciona:

- La investigación *"Diseño de una metodología para la detección de ataques a infraestructuras informáticas basada en la correlación de eventos."* (Pazmiño, 2017), el cual logró determinar que la implementación de su metodología permitia incrementar en un 47,8% la cantidad de detección de ataques informáticos

Por lo que el enfoque de la presente investigación es implementar un correlacionador de eventos que permita aumentar la detección de ataques informáticos basado en software libre.

En la actualidad la red informática de la Empresa Eléctrica RIOBAMBA S.A brinda servicios corporativos en la intranet e internet a usuario finales y público en general, teniendo como principales puntos de su infraestructura el servicio de correo electrónico con aproximadamente 400 cuentas, el servicio de facturación, el firewall corporativo y sistemas financieros. Cabe mencionar que, entre los principales incidentes de seguridad informática detectados por la Dirección de Cómputo, se encuentran los ataques de Denegación de Servicio Distribuido (DDoS) efectuados a la página Web de la EERSA (***http://www.eersa.com.ec/***), así como al sistema de facturación, además de cambios de contraseña en las cuentas corporativas de correo. Sin embargo, en la actualidad la Dirección de Computo de la EERSA no cuenta con una solución centralizada que les permita recolectar, almacenar y gestionar logs provenientes de sus activos de información, con el fin de dar tratamiento a los presentes incidentes informáticos provenientes de sus fuentes de datos.

Justificación

Justificación teórica

En la actualidad, toda empresa oferta servicios en internet, por lo que cualquier problema que interrumpa la disponibilidad de estos, puede llegar a repercutir en indemnizaciones y pérdidas importantes de dinero. Por esta razón la protección de la información debe ser una tarea continua y de mucha importancia, ya que día a día todas las infraestructuras de red son sometidas a cientos de ataques informáticos.

Debido al nivel de complejidad y cantidad de ataques informáticos recibidos en la "Empresa Eléctrica Riobamba S.A", y en general a las que son sometidas las infraestructuras de red, todo intento de vulnerar un sistema genera logs o registros, los cuales quedan almacenados en dichos dispositivos, pero a su vez el procesamiento de toda esta información dispersa podría tomar días o incluso semanas sin contar con el personal y dinero que repercuta para la organización.

Por tal motivo, es indispensable la necesidad de centralizar toda esta información a través de la implementación de un correlacionador de eventos; el cual, a través de la generación de reglas, normalizará y procesará todos estos logs, generando alertas y dándonos a conocer el incidente de seguridad que se está suscitando en tiempo real, de esta manera brindando una respuesta efectiva frente a los incidentes suscitados en la "Empresa Eléctrica Riobamba S.A".

Justificación práctica

Si bien la red informática de la Empresa Eléctrica RIOBAMBA S.A cuenta con una solución de seguridad perimetral que permite mitigar principalmente ataques de denegación de servicio al sistema de facturación, así como spam a los usuarios corporativos, al momento no cuenta con una solución que permita recolectar y almacenar los registros generados por las diferentes capas de seguridad e infraestructura para su posterior análisis y toma de decisiones respecto a seguridad.

En entrevista con personal de la Dirección de Cómputo de la Empresa Eléctrica RIOBAMBA S.A, se determinó la infraestructura general que cuenta con los siguientes equipos: 1 router cisco, 1 firewall checkpoint, 1 swich capa 3 Cisco, entre sus principales equipos; además de varias Vlans, donde se encuentran alojados todos sus servidores y otra Vlan para usuarios.

El correlacionador de eventos será implementado en el segmento de red que contiene los activos de información de la "Empresa Eléctrica RIOBAMBA S.A" y que representen un riesgo para la misma. El correlacionador procesará todos los logs, registros y tráfico de red de los equipos que posean un nivel de riesgo crítico, estos serán enviados mediante mensajes del protocolo SYSLOG, SNMP y capturas de tráfico mediante SPAN.

Formulación del problema

¿Es posible implementar un sistema de detección de ataques informáticos en tiempo real y recolección de logs a infraestructuras de red, basado en la correlación de eventos?

Sistematización del problema

- ¿Cuáles son los sistemas actuales basados en software libre para la detección de incidentes informáticos?
- ¿Cuáles son las ventajas y desventajas de utilizar software libre para la detección de incidentes informáticos?
- ¿Qué riesgos se mitigan al implementar un correlacionador de eventos que permita detectar ataques informáticos?

Objetivos

Objetivo general

Implementar un sistema de recolección y análisis de logs, que permita detectar ataques informáticos, basado en la correlación de eventos en la infraestructura de red de la "Empresa Eléctrica RIOBAMBA S.A".

Objetivos específicos

- Determinar los ataques informáticos que representen un riesgo sobre los activos de información en la infraestructura de red de la "Empresa Eléctrica RIOBAMBA S.A".
- Analizar las diferentes soluciones de detección de ataques informáticos basado en la correlación de eventos OpenSource para su aplicación en el ambiente de producción en la "Empresa Eléctrica RIOBAMBA S.A".
- Implementar un sistema de detección de ataques informáticos basado en la correlación de eventos OpenSource sobre los activos de información críticos del ambiente de producción en la "Empresa Eléctrica RIOBAMBA S.A".

CAPÍTULO I

1. MARCO TEÓRICO

1.1. Ataques Informáticos

En sus inicios, el Internet no era como se lo conoce hoy en día, nació en Estados Unidos con fines militares como el proyecto "ARPANET", el cual consistía en una pequeña red analógica que interconectaba pocos computadores para el intercambio de información, desde ese entonces dicha red de computadores creció de tal manera, hasta convertirse en una gran telaraña que interconecta todo el planeta y que nos brinda servicios como: correo electrónico, páginas web, chat, video llamadas, entre otros. (Hernández, 2000, pp.23-24)

Este crecimiento ha generado nuevas maneras delictivas, en las que, personas con habilidades y conocimientos amplios en el campo informático, utilizan este medio para realizar lo que se conoce como "Ataque Informático" y de esta manera sustraer y apoderarse de información que no les corresponde. Se conoce como ataque informático al aprovechamiento de una debilidad o vulnerabilidad en el software, hardware, en inclusive en las personas que participan en este ambiente. (Mieres, 2009, pp.3-4)

1.1.1 Antecedentes

Siempre que un dispositivo se encuentre interconectado a internet será propenso a sufrir un ataque informático. En la actualidad existen miles de ataques informáticos por día, sin embargo, entre los primeros ataques documentados tenemos al virus "Creeper", el cual afectaba a máquinas IBM 360 que se encontraban en la red "ARPANET", y consistía en emitir un mensaje continuamente en la pantalla que decía: "I'am a creeper….catch me if you can!" (Soy una enredadera, atrápame si puedes). (Borghello, 2006, pp.7)

Entre los mayores ataques informáticos en el mundo podemos mencionar los siguientes:

En Irán, el 27 de septiembre de 2010, los sistemas de control de la Central Nuclear Bushehr, fueron afectados por un virus nunca antes visto denominado "Stuxnet", el cual se apodero de 1000

máquinas que realizaban los procesos de creación de materiales nucleares, modificando el comportamiento en la producción de uranio enriquecido. (Caro, 2010, pp.16-17)

En abril del 2011, PlayStation Network informó a través de su Director, que la información de sus usuarios fue comprometida por un ataque informático que sustrajo: nombres, correos electrónicos y tarjetas de crédito; para contrarrestarlo se desactivaron los servicios temporalmente. (González & Ramírez, 2013, pp.48)

En mayo del 2017 se presentó un ataque masivo en más de 180 países, afectando a más de 360000 computadoras alrededor del mundo llamado "WannaCry", el cual consistía en bloquear y cifrar documentos alojados en la máquina infectada y a su vez se pedía al usuario la cancelación de una suma de dinero, a través de Bitcoins para volver a recuperarlos. (Barros & Pérez, 2017, pp.3-5)

1.2. Fases de un Ataque Informático

Generalmente los ataques informáticos contra las redes de computadoras y sistemas informáticos cuentan principalmente de las siguientes fases:

1.2.1 Reconocimiento

Consiste en realizar un estudio previo, con el fin de obtener la mayor cantidad de información sobre la potencial víctima u objetivo a través de recursos como: Google Hacking, Ingeniería social, Whois, entre otros; es decir en esta etapa casi no se utilizan herramientas de software. La información que se recolecta en esta fase tiene que ver con: rangos de ips, DNS, servidores, servicios. (Benchimol, 2011, pp. 142-146)

1.2.2 Escaneo

En esta fase se utiliza la información previamente obtenida en la etapa de reconocimiento, con el fin de encontrar objetivos de ataque en la infraestructura de red, inicialmente se realiza un escaneo para conocer los puertos abiertos y servicios que se encuentren funcionando en el objetivo, posteriormente se ejecuta un análisis de vulnerabilidades en o los objetivos seleccionados a fin de conocer las vulnerabilidades a nivel de sistema operativo y aplicaciones. (Mieres, 2009, pp. 5)

1.2.3 Acceso

Luego de haber sido encontradas las vulnerabilidades en los objetivos, el siguiente paso es el ingreso al sistema, esto se lo realiza mediante la explotación de una vulnerabilidad a través de un "exploit", el cual puede ser llevado a cabo de forma manual o a través de un sistema de explotación como puede ser: Metasploit Framework, Core Impact, Immunity Canvas, entre otros. Dependiendo del exploit ejecutado es posible interactuar con comandos de sistema operativo como administrador del sistema, caso contrario será necesario escalar privilegios con el fin de obtener control total del mismo. (Benchimol, 2011, pp. 150-153)

1.2.4 Mantenimiento del acceso

En esta fase es importante que el atacante permanezca indetectable para la víctima, para conseguir esto debe eliminar toda evidencia que pudo haber dejado en las fases anteriores y lo más importante hacer uso de un Backdoor o Troyano, para que, al momento de ejecutarlo pueda acceder nuevamente al sistema con privilegios de administrador sin la necesidad de realizar las fases anteriores. (Mamami, 2013, pp. 1–2)

1.3. Tipos de Ataques Informáticos

De acuerdo a la afectación de la característica de disponibilidad, confidencialidad e integridad, la metodología establecida y estandarizada OSSTMM (Manual de la Metodología Abierta de Comprobación de la Seguridad) clasifica ciertos tipos de ataques informáticos en los siguientes grupos:

1.3.1 Denegación de Servicio (Afectación a la Disponibilidad)

Este tipo de ataque informático es conocido como DoS (Denial of Service) y tiene por objetivo la afectación en la disponibilidad de un servicio, consiste en el envío de un número abundante de mensajes hacia la víctima del ataque, de manera que el procesamiento de estos mensajes disminuye los recursos de la víctima hasta agotarlos completamente. (Macía, 2007, pp.35-37)

1.3.2 Phishing (Afectación a la Integridad)

Es un tipo de ataque informático basado en ingeniería social, que tiene por objetivo la extracción de datos confidenciales o información sensible como pueden ser: contraseñas, tarjetas de crédito, entre otras; mediante el engaño al usuario a través de la suplantación de identidad de fuentes confiables. El éxito del ataque radica en la falta de conocimiento y comprensión de la víctima en sistemas informáticos. (Belisario, 2014, pp.8-10)

1.3.3 Ataques de Inyección de código SQL (Afectación a la Integridad, Confidencialidad)

Se considera como uno de los ataques informáticos de mayor criticidad, ya que permite realizar consultas y ejecución de código SQL directamente entre el cliente y el aplicativo WEB, si el ataque fue exitoso, el atacante podría extraer la estructura de las bases de datos, realizar consultas sobre tablas, insertar, modificar o eliminar información. Una Inyección SQL se produce cuando el código del aplicativo WEB no realiza una correcta validación de los parámetros enviados desde el usuario. (Gómez, 2014, pp. 5)

1.3.4 Cross Site-Scripting (XSS) (Afectación a la Integridad, Confidencialidad)

Este tipo de ataques informáticos se los realiza contra aplicaciones Web, tiene por objetivo tomar el control sobre el navegador que utiliza un usuario y de esta manera ejecutar scripts maliciosos (generalmente en HTML o JavaScript) que permitan robar información confidencial como son las cookies e identificadores de sesión. (Alfaro, 2007, pp. 1-2)

1.3.5 Fuerza Bruta (Afectación a la Confidencialidad)

El objetivo de este ataque informático es descubrir la contraseña de un usuario o servicio de manera agresiva, ya sea probando todas las combinaciones posibles hasta obtener el acceso. Generalmente este ataque se combina con un ataque de diccionario, para lo cual, el éxito dependerá de la cantidad de palabras previamente almacenadas por el atacante. (Bahit, 2012, pp. 1-4)

1.3.6 Mail Spoofing (Afectación a la Integridad, Disponibilidad)

Este ataque informático consiste en la suplantación de identidad de un usuario de correo, con el fin de enviar grandes cantidades de e-mails para de esta manera sustraer información confidencial de sus víctimas, dicho ataque generalmente viene acompañado con técnicas de phishing. (Telefónica, 2017, pp. 2-4)

1.4. Security Information and Event Management Systems (SIEM)

En los últimos años los ataques informáticos a infraestructuras de red ha crecido vertiginosamente, para hacer frente a dichos ataques las organizaciones se centran en gestores de seguridad de la Información y Gestión de Eventos (SIEM), los mismos que ayudan en la defensa de arquitecturas a través de la correlación centralizada de eventos (Pedroza, 2016, pp. 15)

1.4.1 Antecedentes

Un SIEM es la combinación de tecnologías SEM y SIM, con el objetivo de beneficiar a los analistas de seguridad y administradores, a través de la recepción de eventos de red, brindando de esta manera una visión del entorno donde se encuentra instalado.

El Security Event Manager SEM posee las siguientes características:

- Recopilación de datos y eventos
- Visualización de eventos a través del control dinámico de la consola
- Monitoreo en tiempo real
- Gestión de eventos

Mientras que el Security Information Manager SIM, se encarga de:

- Presentación de informes de eventos de seguridad
- Análisis histórico (repositorio de datos)

Un sistema de correlación de eventos está conformado por 4 capas, como se detalla en la figura 1-1.

Figura 1-1: Capas de un Sistema SIEM
Fuente: (AlienVault Academy, 2014)

1.4.1.1 Capa de recolección de eventos

Su función es recolectar todos los eventos que son generados por los dispositivos de red o de seguridad como se muestra en la figura 2-1.

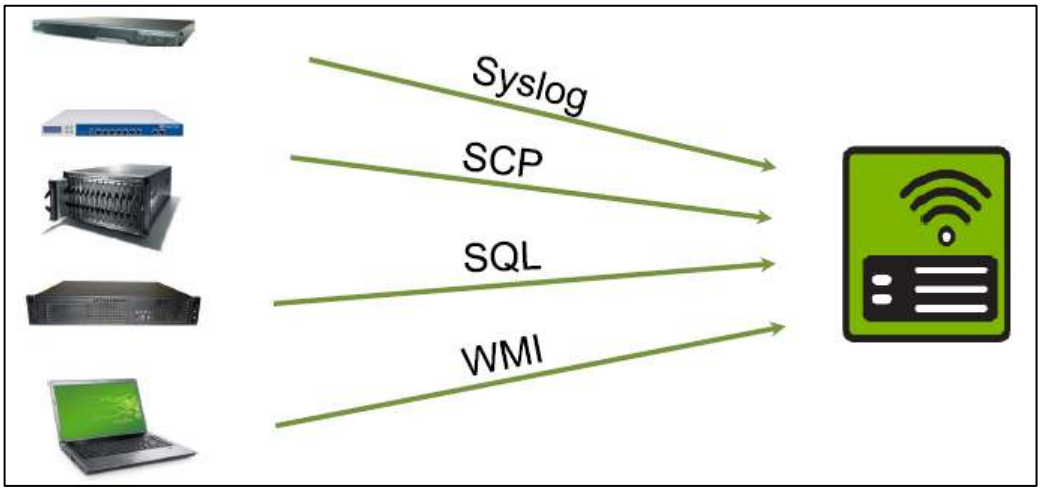


Figura 2-1: Capa de Eventos
Fuente: (AlienVault Academy, 2014)

1.4.1.2 Capa de normalización

Su objetivo es estandarizar todos los eventos que son recibidos en el SIEM, de manera que una vez finalizado este proceso posean el mismo formato de datos y puedan ser enviados a la capa de correlación.

En la figura 3-1, se muestra un ejemplo de autenticación fallida, desde diferentes dispositivos y el proceso que realiza la capa de normalización, con el fin de estandarizar los logs en un mismo formato.

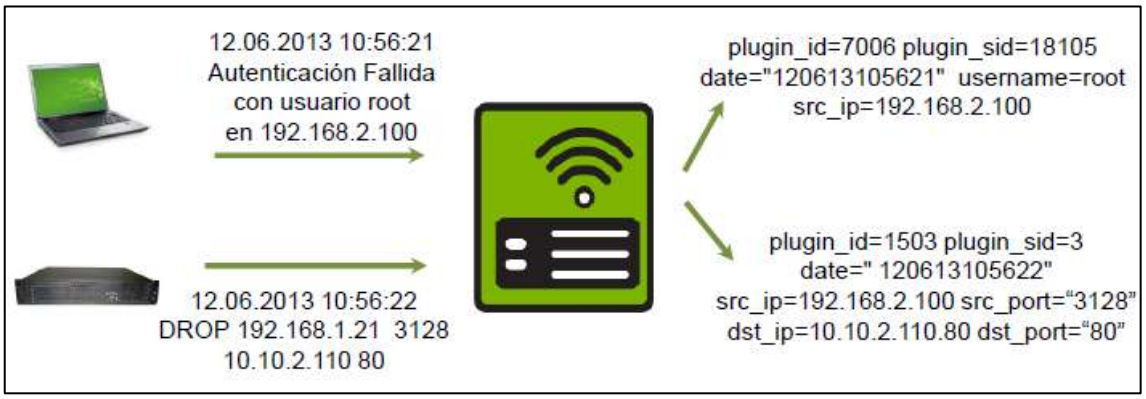


Figura 3-1: Capa de normalización
Fuente: (AlienVault Academy, 2014)

1.4.1.3 Capa de correlación

Su función es determinar parámetros en común, de los registros y logs anteriormente ya normalizados.

De acuerdo con la figura 4-1, se muestran intentos repetitivos de autenticación SSH, desde el origen X al destino Y, para lo cual la capa de correlación puede tratar este comportamiento de manera que establezca patrones de incidencia y lo catalogue como un ataque de fuerza bruta.

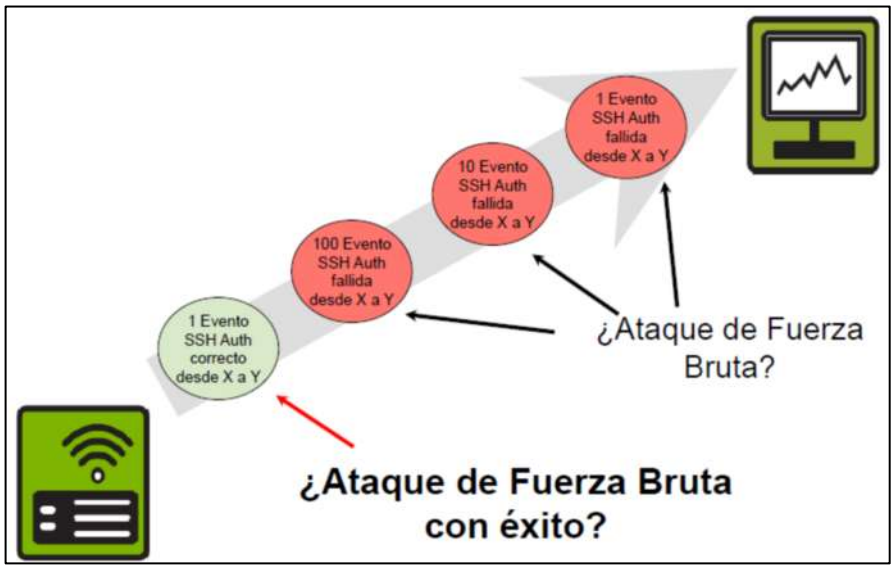


Figura 4-1: Capa de Correlación
Fuente: (AlienVault Academy, 2014)

1.4.1.4 Capa de reporte

De acuerdo con la figura 5-1, la función de la capa de reporte es analizar los resultados previamente enviados por la capa de correlación, procesándolos y generando informes sobre los eventos que suceden en los dispositivos de red.

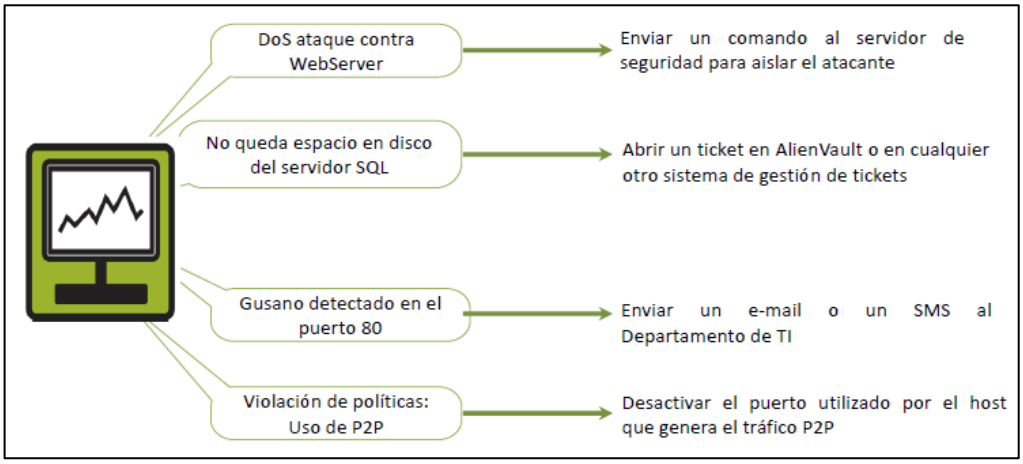


Figura 5-1: Capa de reporte, acciones correctivas
Fuente: (AlienVault Academy, 2014)

Para un análisis más detallado, es necesario la generación de informes, con diagramas de barras, histogramas y gráficos, como se muestra en la figura 6-1.

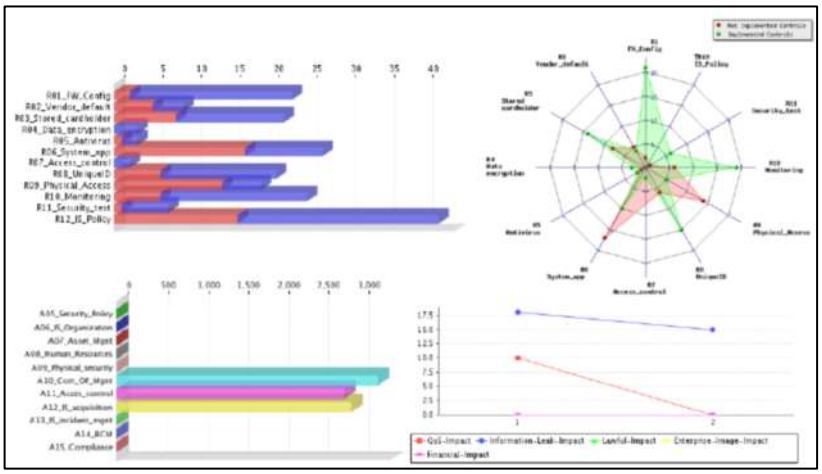


Figura 6-1: Capa de reporte, generación de informes
Fuente: (AlienVault Academy, 2014)

1.5. Arquitecturas de Seguridad Informática Estratificada

El enfoque de seguridad estratificada se centra en mantener medidas y procedimientos de seguridad adecuados en cinco capas diferentes dentro de un entorno de TI, las cuales son: datos, aplicaciones, host, red y perímetro.

La implementación de seguridad en capas permite garantizar los principios de integridad, confidencialidad y disponibilidad de extremo a extremo. (Kannan, 2014, http://opensourceforu.com/2014/02/top-10-open-source-security-tools/)

1.5.1 Seguridad de los datos

Esta sección cubre herramientas de cifrado para proporcionar confidencialidad a nivel de datos. Cifrar los datos que residen en el sistema local e incluso cuando se desplaza por la red es una buena práctica recomendada porque, si todas las otras medidas de seguridad fallan, un esquema de cifrado robusto será el último control mitigante de seguridad.

1.5.2 Seguridad de la aplicación

La seguridad de la aplicación es tan importante como las demás capas de la arquitectura. Cada día hay un aumento drástico de compañías para desarrollo de aplicaciones y plataformas web. De manera similar, las vulnerabilidades web también están aumentando, y la mayoría de las vulnerabilidades se descubren después de la implementación. La razón principal de las amenazas a la seguridad de las aplicaciones, es que los aspectos de seguridad no se tienen en cuenta durante el diseño y desarrollo de las mismas. (Kannan, 2014, http://opensourceforu.com/2014/02/top-10-open-source-security-tools/)

1.5.3 Seguridad de host

La seguridad a nivel de host protege los dispositivos individuales, como servidores, computadoras de escritorio, portátiles, etc. dentro de la red. Se trata de gestionar herramientas que proporcionen seguridad en el nivel de host, porque están diseñadas para cumplir con las características específicas de un solo dispositivo.

1.5.4 Seguridad a nivel de red

La seguridad a nivel de red está entre las más importantes, ya que esta capa se encarga del enrutamiento y conmutación de paquetes. El esquema de direccionamiento utilizado en este nivel son las direcciones IP, y el dispositivo que centraliza el manejo del tráfico es el router. Por lo tanto en esta capa es evidente la necesidad de una respuesta activa ante la intención del atacante, al suplantar un paquete e indicar que proviene de otro sistema.

1.5.5 Seguridad Perimetral

El perímetro de seguridad es el área donde termina la red y comienza Internet. El perímetro consiste en uno o más firewalls que filtran flujos de datos entre los diferentes clientes de una organización y los recursos disponibles que son alcanzados mediante Internet.

Las herramientas de IDS(Sistema de Detección de Intrusos) alertan al personal de TI al momento de recibir un ataque; las herramientas IPS(Sistema de Prevención de Intrusos) van un paso más allá y bloquean automáticamente el tráfico malicioso. Por tal motivo los IPS e IDS cumplen papel importante en la arquitectura de seguridad de una organización.

1.5.6 Gestión de Vulnerabilidades

La gestión de vulnerabilidades es una práctica de seguridad diseñada para prevenir proactivamente la explotación de las debilidades informáticas que existen dentro de la organización. La administración de vulnerabilidades por sí sola no mitiga el nivel de riesgo, para ello es necesario la gestión de parches, configuraciones, software antivirus, políticas, procedimientos y normativas de seguridad para la gestión de activos de información. (Kannan, 2014, http://opensourceforu.com/2014/02/top-10-open-source-security-tools/)

1.6. Tipos de Soluciones SIEM opensource

1.6.1 OSSIM

OSSIM(Open Source Security Information y Event Management) es una herramienta opensource que permite tratar la información generada, almacenarla y priorizarla mediante técnicas de correlación, de modo que se pueda proporcionar una visibilidad global, de los incidentes en los sistemas y tratar esta información con un formato unificado, OSSIM nos permitirá priorizar los incidentes según la criticidad en que se produzcan, de manera que sea posible monitorizar el estado de seguridad de la red. (Párrizas, 2005, pp.39)

Permite además integrar la información generada por IDSs, monitores de tráfico de red, Firewalls y dispositivos de análisis, con la posibilidad de realizar un inventario de todos los activos, definir la topología de red, establecer políticas de seguridad, etc.(AlienVault Academy, 2014)

1.6.1.1 Funciones principales de OSSIM:

Pre-proceso: se trata en detectar y generar alertas por parte de los detectores, para afianzar el proceso de enviar información.(AlienVault Academy, 2014)

Colección: en esta parte los detectores envían toda la información recibida, a un servidor central.

Post-proceso: se realiza el tratamiento de la información recibida en su totalidad, una vez que se encuentre centralizada.

La fase de Post-proceso incluye tres métodos diferentes:

- *Priorización:* se crea una Política Topológica de Seguridad y un Inventariado de los sistemas, de manera que se establecen métricas que permiten clasificar los niveles de las alertas recibidas.
- *Valoración de Riesgo:* según el riesgo valorado para cada evento y de una forma proporcional al activo al que se aplica, se puede suponer un nivel de amenaza y la probabilidad para que el incidente se materialice.(Muñoz et al, 2003, pp.1-34)
- *Correlación:* para obtener una información de mayor significancia, se analiza un conjunto de incidentes registrados.

Así pues, las alertas ofrecidas por los detectores, después de ser tratadas, pasarán a ser alarmas o no según sea el caso. El resultado del proceso de varias alertas se considera como una alarma y consigue un nivel superior de conceptualización y de fiabilidad.(Párrizas, 2005, pp. 40)

1.6.2 AlienVault SIEM

La compañía AlienVault fue fundada por los creadores de OSSIM en España durante el año 2007, es un producto de información de seguridad de código abierto y gestión de eventos. AlienVault combina los componentes tales como Sensor, Logger y Server. (AlienVault Academy, 2014)

1.6.2.1 Componentes de AlienVault

- *Sensor*

El sensor AlientVault se encarga de recoger los incidentes generados en la red, independientemente a que este tráfico, sea generado por sus aplicativos internos. Frente a un evento, es el encargado de generar un reporte normalizado que se envía al Server o al Logger para su procesamiento. AlienVault puede tener tantos sensores como sea necesario. Se conocerá como Origen de Datos o Data Source a cualquier tecnología que genere información y permita la llegada al Sensor de AlientVault. (Pazmiño, 2017, pp. 41)

En la figura 7-1, se muestra una pequeña lista de los clientes estandarizados de AlientVault.

Figura 7-1: AlienVault clients
Fuente: (AlienVault Academy, 2014)

Como plugins o tipos de conectores disponibles para AlienVault se puede considerar:

- *Detectores*: De acuerdo al Manual Oficial de AlienVault, los detectores "son orígenes de datos, sin embargo, aportan eventos como Snort, Firewalls, Antivirus, Web servers, Sistemas Operativos, etc"

En la figura 8-1 se muestra un ejemplo de un componente detector de Sistema Operativo.

```
Mar 13 05:14:55 ossim  sshd[11571]: Accepted password for root from 192.168.1.36 port 53328 ssh2
Mar 13 05:14:55 ossim  sshd[11579]: (pam_unix) session opened for user root by root(uid=0)
Mar 13 05:14:55 ossim  sshd[11586]: (pam_unix) session opened for user root by (uid=0)
Mar 13 05:14:55 ossim  sshd[11588]: (pam_unix) session opened for user munin by root(uid=0)
```

Figura 8-1: Ejemplo de un componente detector de S.O
Fuente: (AlienVault Academy, 2014)

- *Monitores:* Es un conjunto de herramientas tales como Webs, Nmap, Tcptrack, Ntop, Compromise & Attack, entre otras. La cuales se encargan de gestionar la red, para generar indicadores del comportamiento y estadísticas de tráfico.

En la figura 9-1 se muestra un ejemplo de un componente monitor de Sistema Operativo.

Client	Server	State	Idle	A Speed
172.23.195.11:48328	63.39.22.44:22	ESTABLISHED	0s	38 KB/s
172.23.195.11:48646	63.39.22.44:22	ESTABLISHED	1s	30 KB/s
172.23.195.11:48661	63.39.22.44:22	ESTABLISHED	0s	307 B/s
172.23.195.11:48620	63.39.22.44:22	RESET	2s	0 B/s
128.230.225.95:3531	63.39.22.44:22	ESTABLISHED	5s	0 B/s
172.23.195.11:48321	63.39.22.44:22	ESTABLISHED	7s	0 B/s
TOTAL				69 KB/s
Connections 1-6 of 6			Unpaused	Sorted

Figura 9-1: Ejemplo de un componente monitor de S.O
Fuente: (AlienVault Academy, 2014)

Tal como se muestra en la figura 10-1, el sensor de AlienVault puede agregar eventos utilizando múltiples métodos de recolección.

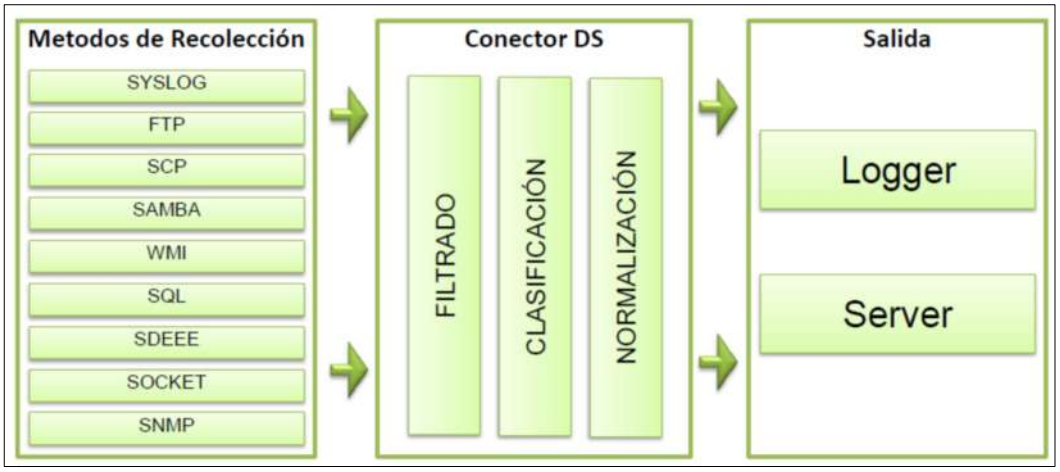


Figura 10-1: Data Source AlienVault
Fuente: (AlienVault Academy, 2014)

- *Logger*

Para su administración, Logger incluye una Consola Web y utiliza una base de datos MySQL (Percona). Para realizar un análisis forense, AlienVault Logger permite recoger y archivar un número ilimitado de datos, únicamente dependiendo del tamaño del disco duro y su capacidad para almacenamiento, aunque la versión Enterprise tiene la posibilidad de hacerlo en un servidor NAS o SAN. Este componente por sus características es una pieza fundamental en implementaciones que deben cumplir una política internacional específica.(Pazmiño Gómez, 2017)

De acuerdo con el Manual Oficial de AlienVault, indica que el almacenamiento de los eventos se los debe realizar en formato RAW en el file system o sistema de archivos, los incidentes están firmados digitalmente y almacenados masivamente para asegurar su admisión, como prueba ante un tribunal de justicia o respaldo legal.

- *Server*

Server es el encargado de procesar los datos recolectados por los sensores y dispositivos de red, también puede aprovechar el inventario creado por sus sensores AlienVault, así como de bases de datos externas para amenazas informáticas y la Correlación cruzada de los eventos, para eliminar lo que se conoce como falsos positivos y ofrecer un procesamiento más analítico. (Pazmiño Gómez, 2017)

El componente SIEM proporciona al sistema la Inteligencia de Seguridad y capacidades de evaluación tales como:

- Evaluación del riesgo
- Correlación
- Métricas de Riesgo
- Escaneo de Vulnerabilidades
- Monitoreo en tiempo real de los eventos

La figura 11-1 muestra el flujo de procesamiento de los eventos en el SIEM.

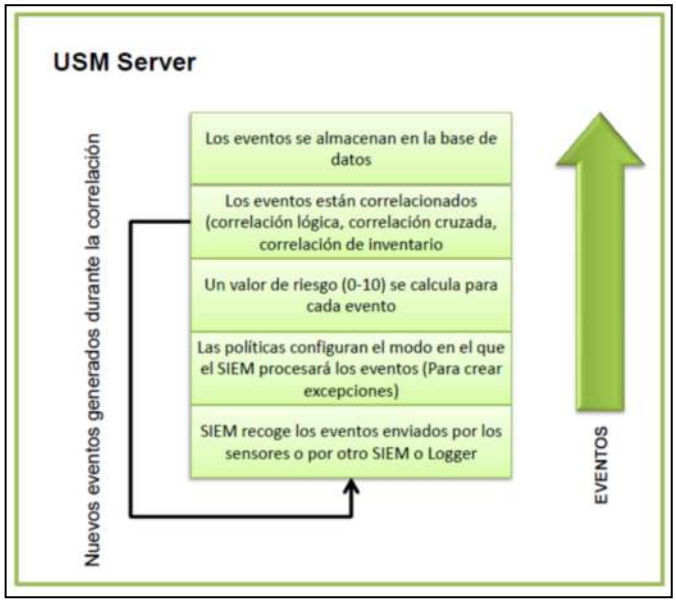


Figura 11-1: Procesamiento de los eventos en el SIEM
Fuente: (AlienVault Academy, 2014)

1.6.3 Security Onion

Security Onion es una distribución open source, basada en Ubuntu, que recopila un gran número de herramientas destinadas al análisis forense, tanto de redes como de sistemas, de manera que se pueda garantizar el correcto funcionamiento de los componentes y la inexistencia de todo tipo de intrusos en la red.

Security Onion posee una gran variedad de paquetes y herramientas por defecto, para auditar la seguridad de todo tipo de redes. (Burks, 2017, https://github.com/Security-Onion-Solutions/security-onion/wiki)

En la estructura de seguridad tenemos tres funciones principales, que vienen enlazadas entre sí:

- Captura de tráfico
- Sistemas de detección de intrusos basados en la red y en el host (NIDS y HIDS, respectivamente)
- Suite de poderosas herramientas de análisis.

1.6.3.1 Captura de tráfico

La captura completa de tráfico, se realiza a través de netsniff-ng (http://netsniff-ng.org/), netsniff-ng captura todo el tráfico que llega a los sensores de Security Onion y almacena tanto tráfico como este configurado y pueda soportar (Security Onion tiene un mecanismo incorporado para purgar datos viejos antes de que sus discos se llenen en toda su capacidad). (Burks, 2017, https://github.com/Security-Onion-Solutions/security-onion/wiki)

1.6.3.2 Sistemas de Detección de Intrusos (HIDS/NIDS)

Los sistemas de detección de intrusión (IDS) basados en la red y en el host, analizan el tráfico de la red o los sistemas host, respectivamente, y proporcionan datos de registro y alerta para detectar eventos y actividades.

Security Onion proporciona múltiples opciones de NIDS, los cuales se muestran en la tabla 1-1.

Tabla 1-1: Sistemas de Detección de Intrusos basados en Red (NIDS)

NIDS	SNORT	BRO NETWORK SECURITY MONITOR	SURICATA
BASADOS EN REGLAS	El sistema basado en reglas analiza el tráfico de la red en busca de rastros e identificadores que coincidan con el tráfico malicioso, anómalo o sospechoso. Podría decir que son similares a las firmas de antivirus, pero son más profundas y más flexibles que eso.		Suricata es un NIDS más joven, de código libre y rápido, aunque en fase de desarrollo. Inspecciona el tráfico de la red utilizando reglas potentes y muy extensas, tiene un poderoso soporte de secuencias de comandos

BASADO EN ANÁLISIS		Bro supervisa la actividad de la red y registra conexiones, solicitudes de DNS, software y servicios de red detectados, certificados SSL y HTTP, FTP, IRC SMTP, SSH, SSL y Syslog actividad que ve, proporcionando una profundidad real y visibilidad en el contexto de datos y eventos en su red.	Lua para la detección de amenazas complejas, y diseñado para trabajar con los conjuntos de reglas de Snort.

Realizado por: Pazmiño, J; Pazmiño, C. 2018

- *HIDS*

Para la detección de intrusiones basada en host, Security Onion ofrece OSSEC Originalmente creado por Daniel Cid, Trend-Micro adquirió OSSEC en 2009 y continúa ofreciéndolo como una solución de código abierto. Como analista, la capacidad de correlacionar eventos basados en host y en la red puede ser la diferencia para identificar un ataque exitoso. (Burks, 2017, https://github.com/Security-Onion-Solutions/security-onion/wiki)

1.6.3.3 Suite de Herramientas de Análisis

Con la captura completa de paquetes, los registros de IDS y los datos de Bro, existe una enorme cantidad de datos disponibles a clasificar y manipular por el analista. Afortunadamente, Security Onion integra las siguientes herramientas para ayudar a dar sentido a estos datos:

- *Sguil*

Disponible en (http://sguil.sourceforge.net/) creado por Bamm Visscher. Es la consola de seguridad para el monitoreo de red. Proporciona visibilidad de los eventos que fueron recopilados y el contexto del ataque para validar la detección. Más importante aún, Sguil permite la redirección directa de una alerta a un paquete capturado (a través de Wireshark o NetworkMiner) para realizar un análisis más a fondo y completo del tráfico que activo la alerta.

Sguil se diferencia de otras interfaces de alerta en que permite la colaboración entre analistas al permitir que las alertas sean comentadas y escaladas a más analistas senior que pueden tomar

medidas sobre los incidentes. (Burks, 2017, https://github.com/Security-Onion-Solutions/security-onion/wiki)

En la figura 12-1 se muestra la interfaz de la aplicación Web de Sguil.

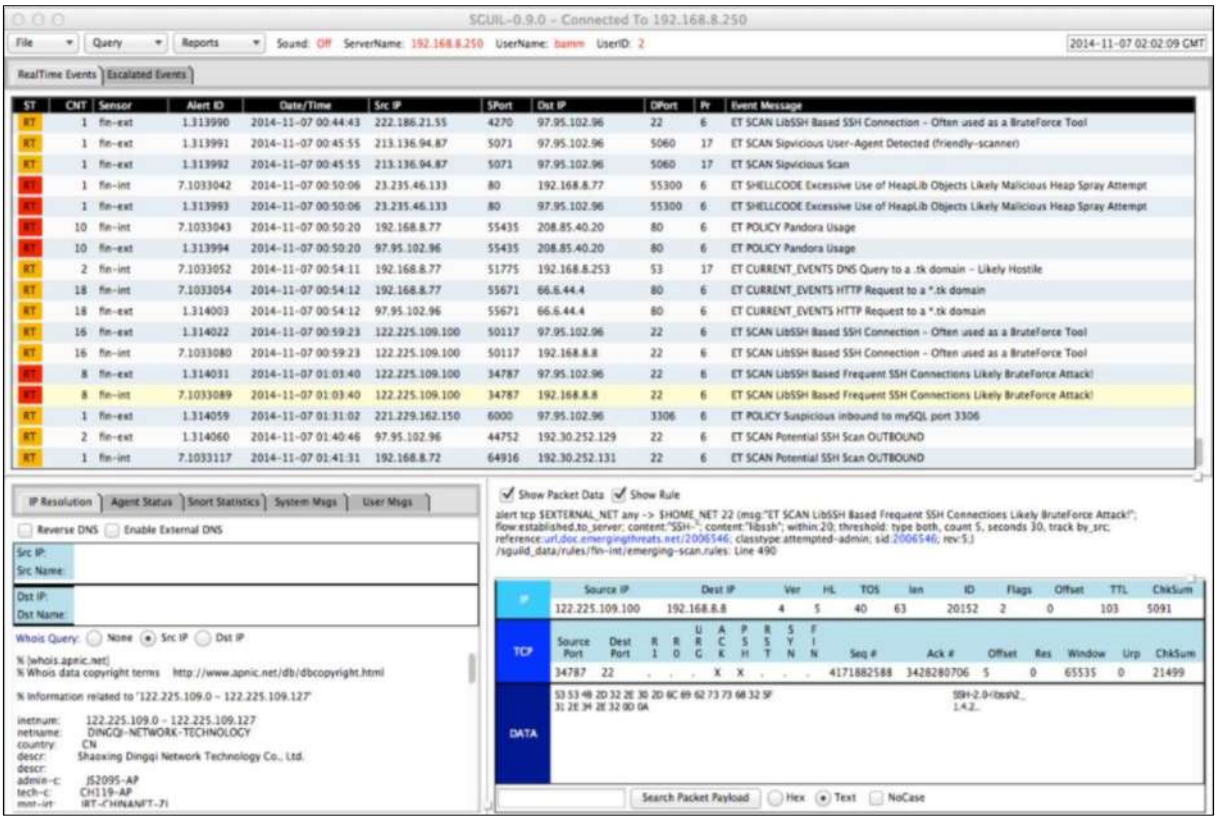


Figura 12-1: Interfaz de Sguil para la administración de eventos
Fuente: http://bammv.github.io/sguil/images/sguil_main.png

- *Squert*

Disponible en (http://www.squertproject.org/), creado por Paul Halliday, es una interfaz de aplicación web que se utiliza para consultar y visualizar datos de eventos almacenados en la base de datos Sguil. Squert es una herramienta visual que intenta proporcionar un contexto adicional a los eventos a través del uso de metadatos, representaciones de series de tiempo y conjuntos de resultados ponderados y agrupados lógicamente. (Burks, 2017, https://github.com/Security-Onion-Solutions/security-onion/wiki)

En la figura 13-1 se muestra la interfaz de la aplicación Web de Squert.

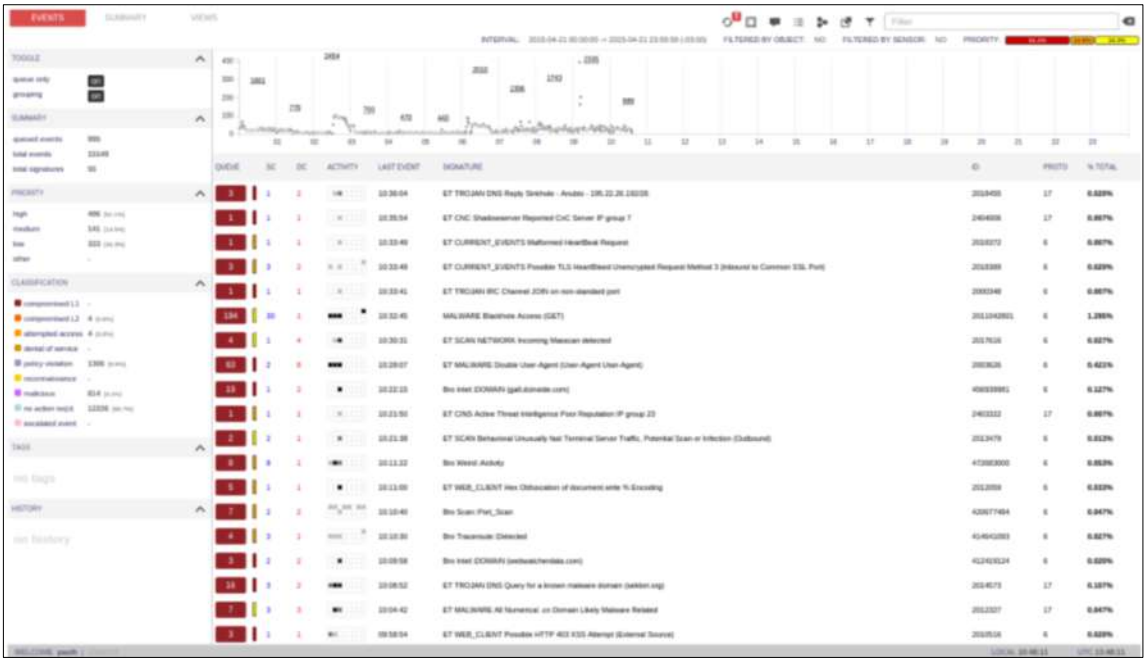


Figura 13-1: Cola de alertas en la pestaña de eventos
Fuente: http://www.squertproject.org/

Se ha creado un filtro para la búsqueda de eventos relacionados con virus “troyanos” y eventos actuales relacionados con el tema, tal como se muestra en la figura 14-1.

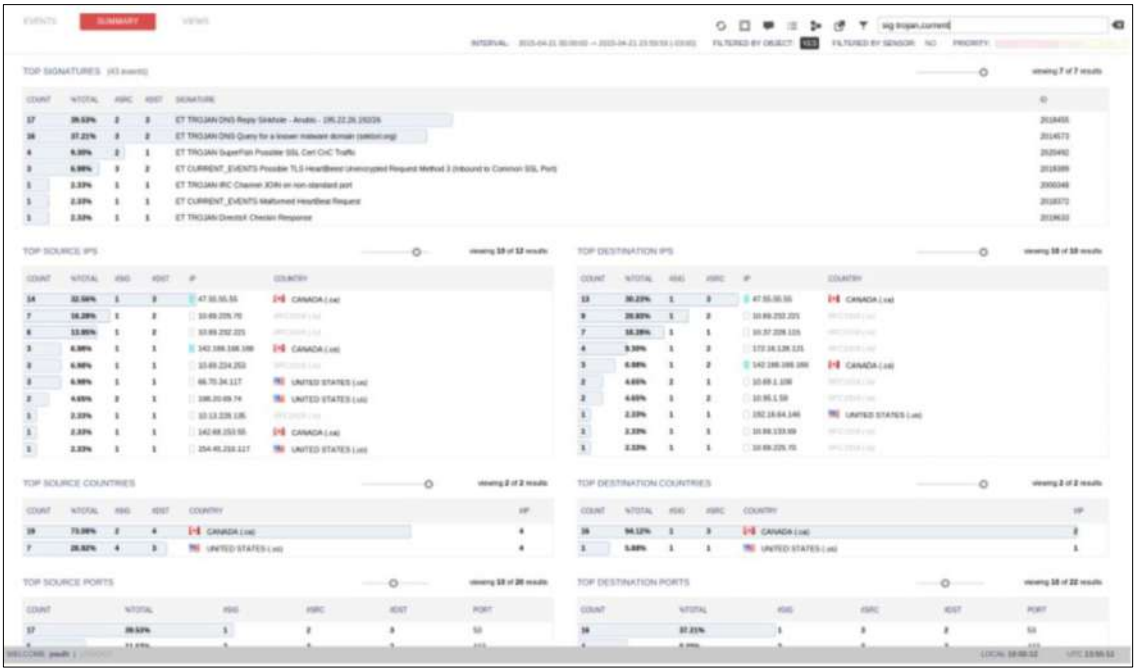


Figura 14-1: Filtrado para "troyano" y "eventos actuales" en la página de resumen.
Fuente: http://www.squertproject.org/

1.7. OSSEC

OSSEC (Open Source Secure) es una plataforma para monitorear y controlar sistemas informáticos. Combina todos los aspectos de un HIDS (detección de intrusiones basada en host), monitoreo de registros, y gestión de incidentes de seguridad / gestión de eventos de seguridad (SIM / SEM). La adopción de OSSEC por parte de la industria de TI está creciendo rápidamente, por ser una solución de código abierto simple y potente. (OSSEC, 2017, https://ossec.github.io/docs/manual/)

Las características importantes de OSSEC:

- Comprobación de integridad de archivos
- Monitorización de registros
- Detección de Rootkit
- Respuesta activa
- Seguridad de la red

1.7.1 Beneficios clave de OSSEC

1.7.1.1 Multi plataforma

OSSEC permite a los clientes implementar un sistema integral de detección de intrusos basado en host con políticas específicas de aplicaciones / servidores en múltiples plataformas como Linux, Solaris, Windows y Mac OS X.

1.7.1.2 Alertas configurables y en tiempo real

OSSEC permite a los clientes configurar los incidentes en los que desean recibir alertas y les permite aumentar la prioridad y concentrarse en los incidentes de mayor criticidad sobre el tráfico habitual en cualquier sistema. La integración con smtp, sms y syslog permite a los clientes estar al tanto de las alertas enviándolas a dispositivos habilitados para el reporte mediante correo electrónico.

1.7.1.3 Integración con la infraestructura actual

OSSEC se integra con versiones actuales de SIM/SEM (gestión de incidentes de seguridad/gestión de eventos de seguridad) para la generación de informes centralizados y la correlación de eventos.

1.7.1.4 Gestión centralizada

OSSEC proporciona un servidor de administración centralizado y simplificado que permite administrar políticas en múltiples sistemas operativos. Además, permite a los clientes definir configuraciones específicas del servidor para la gestión políticas detalladas. (OSSEC, 2017, https://ossec.github.io/docs/manual/)

1.7.2 Arquitectura OSSEC

De acuerdo con la figura 15-1, OSSEC está compuesto de múltiples elementos. Tiene un administrador central para supervisar y recibir información de agentes, syslog, bases de datos y dispositivos sin agente.

Figura 15-1: Arquitectura de Ossec
Fuente: https://ossec.github.io/docs/manual/ossec-architecture.html

1.7.2.1 Servidor

El servidor es el elemento central de la implementación de OSSEC. Almacena los registros de ingreso al sistema, las bases de datos, los eventos y las entradas de auditoría. Todas las reglas, decodificadores y sus principales opciones de configuración se almacenan centralmente en el servidor; por lo que es fácil administrar incluso una gran cantidad de agentes.(OSSEC, 2017)

Los agentes se conectan al servidor mediante el puerto 1514/udp. La comunicación a este puerto debe permitirse para que se pueda establecer un flujo de datos bidireccional.

1.7.2.2 Agentes

El agente es un programa pequeño, o un conjunto de sub-programas instalado en los sistemas que se supervisarán. El agente recopilará información y la reenviará al servidor para su análisis y correlación. Parte de la información se recopila en tiempo real, otras periódicamente.

Nota: En las plataformas bajo sistema operativo Microsoft Windows, solo se puede instalar OSSEC como un agente. Los registros generados en forma de logs, deberán ser procesados por un servidor OSSEC, que se ejecute en Linux u otro sistema operativo similar a Unix.

1.7.2.3 Sin agente

Para sistemas en los que no se puede instalar un agente, el soporte sin agente puede permitir que se realicen comprobaciones de integridad. Los escaneos sin agente se pueden usar para monitorear firewalls, enrutadores e incluso sistemas Unix. (OSSEC, 2017, https://ossec.github.io/docs/manual/)

1.7.2.4 Comunicación entre agentes y el servidor OSSEC

Para la comunicación entre los agentes y el servidor OSSEC generalmente se utiliza el puerto 1514/UDP en modo seguro. Si se usa el modo syslog para ossec-remoted, entonces se utilizará el puerto 514 (tanto UDP como TCP son compatibles). Estos puertos son configurables en el archivo ossec.conf.

Siempre que sea posible, se recomienda utilizar el método de conexión segura en lugar a syslog. Además, se puede usar un daemon syslog externo (como rsyslog o syslog-ng) en lugar del soporte syslog enossec-remoted. (OSSEC, 2017, https://ossec.github.io/docs/manual/)

1.8. ELASTIC STACK

Se denomina Elastic Stack al conjunto de tecnologías compuestas por Elasticsearch, Logstash y Kibana (ELK). Además se ha incorporado lo que elastic ha bautizado como X-pack, que es una especie de combinado de herramientas con diferentes funciones como alertas, seguridad, reportes, monitoreo, etc. (Burks, 2017, https://github.com/Security-Onion-Solutions/security-onion/wiki)

1.8.1 Requisitos de hardware

Los requisitos mínimos para la implementación de ELK son:

- 2 núcleos de CPU
- 8GB de RAM

1.8.2 Arquitectura Security Onion con Elastic Stack

De acuerdo con la figura 16-1, se muestra la arquitectura propuesta de Security Onion con soporte de Elastic Stack. En la cual constan los componentes principales y secundarios de ELK.

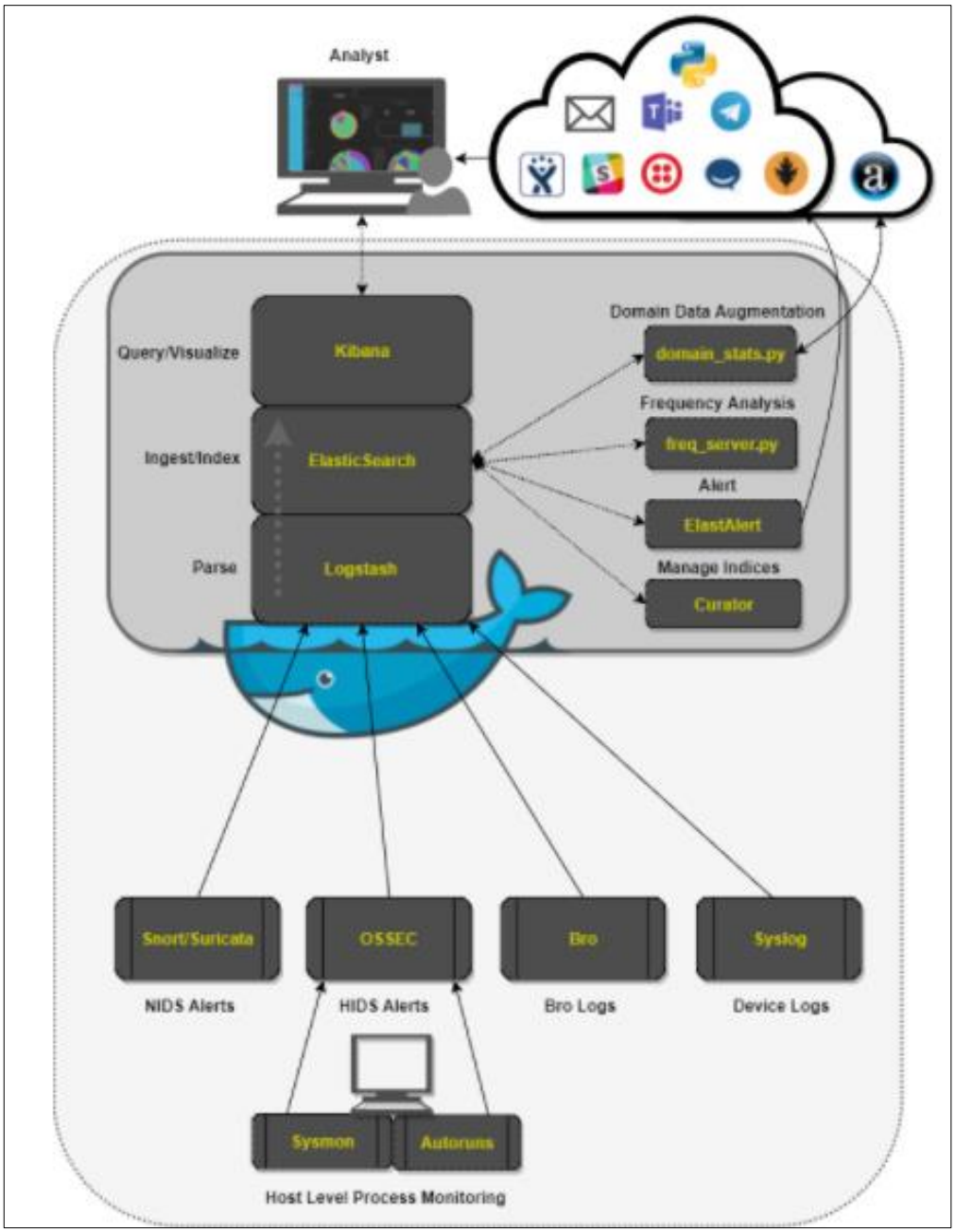


Figura 16-1: Diagrama de arquitectura de alto nivel – Componentes Principales y Secundarios de Elastic Stack
Fuente: https://github.com/Security-Onion-Solutions/security-onion/wiki/Elastic-Architecture

1.8.3 Arquitectura Elastic Stack

En la figura 17-1 se muestra un diagrama de funcionamiento de la plataforma de administración de logs, Elastic Stack, conformada por Logstash, Elasticsearch y Kibana. Donde es posible reconocer las fases de recolección de logs, almacenamiento y visualización.

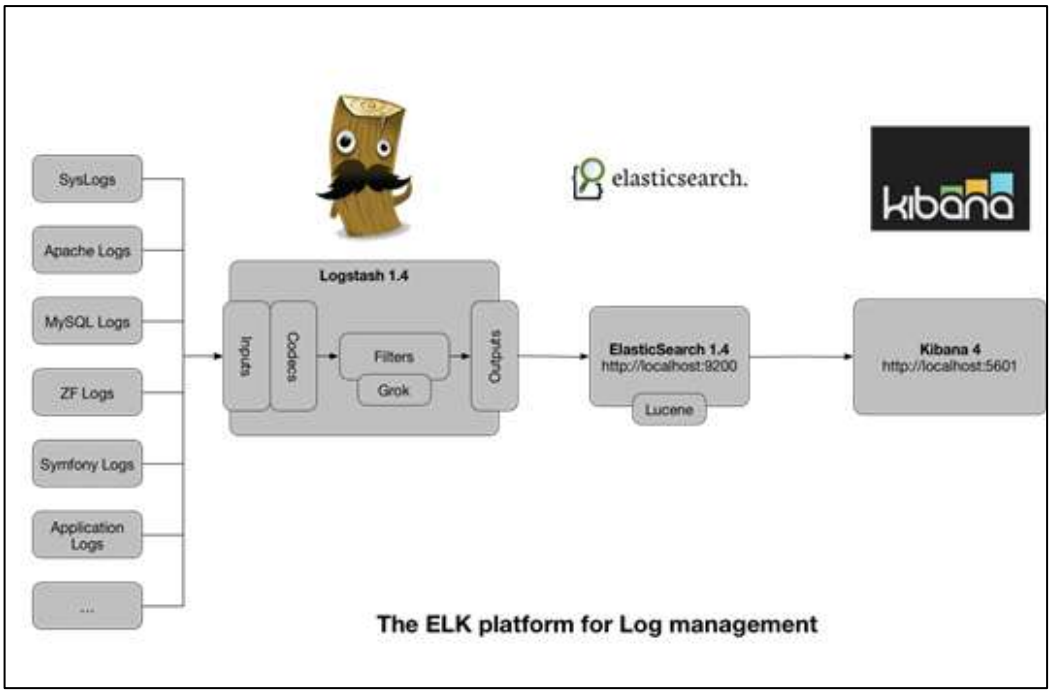


Figura 17-1: Arquitectura ELK para plataformas de logs
Fuente: https://www.elastic.co/blog/psd2-architectures-with-the-elastic-stack

1.8.4 Componentes Principales de Elastic Stack

1.8.4.1 Logstash

Es un servicio de código abierto que se encarga de la canalización dinámica de información y recopilación de datos, normalmente logs, los procesa y los transforma en información que se puede almacenar y mostrar de manera más humana en Elasticsearch.

1.8.4.2 Elasticsearch

Es un motor de búsqueda y análisis distribuido (que permite utilizar un procesador que no es el local para realizar trabajos que requieren un gran consumo de procesamiento.). Considerado una pieza fundamental de Elastic Stack ya que se encarga de almacenar y realizar búsquedas de información en grandes volúmenes de datos, de manera muy rápida, basado en JSON(JavaScript Object Notation, es un formato de texto ligero para el intercambio de datos.), diseñado para máxima confiabilidad y administración fácil.

1.8.4.3 Kibana

Nos permite visualizar los datos almacenados en Elasticsearch y navegar por Elastic Stack, de modo que se pueda dar forma a los datos de manera personalizada, en pocas palabras es la interfaz de usuario que sirve para configurar y administrar todos los aspectos de Elastic Stack.

X-Pack es una extensión única que integra funciones útiles: seguridad, alertas, monitoreo, informes, exploración de gráficos y aprendizaje automático. (Burks, 2017, https://github.com/Security-Onion-Solutions/security-onion/wiki)

1.8.5 Componentes Auxiliares de Elastic Stack

En la figura 18-1 se muestra los componentes auxiliares de Elastic Stack.

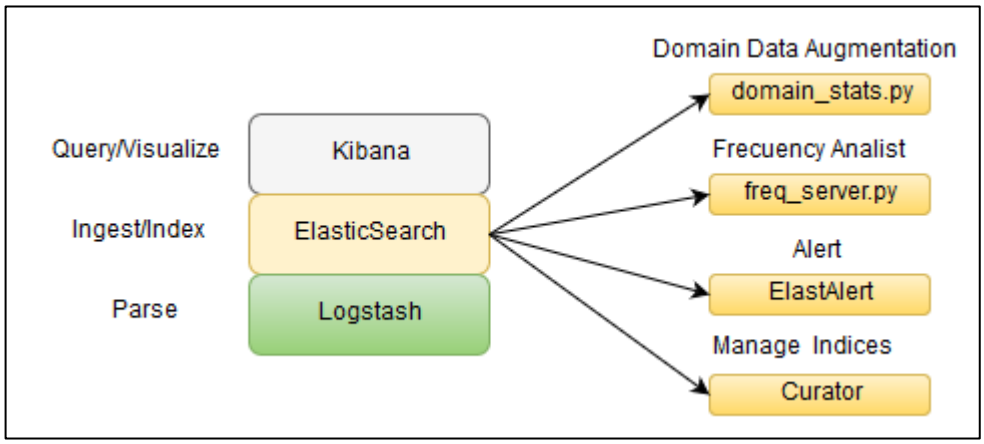


Figura 18-1: Componentes Auxiliares de Elastic Stack
Fuente: https://github.com/Security-Onion-Solutions/security-onion/wiki/Elastic-Architecture

1.8.5.1 Curator

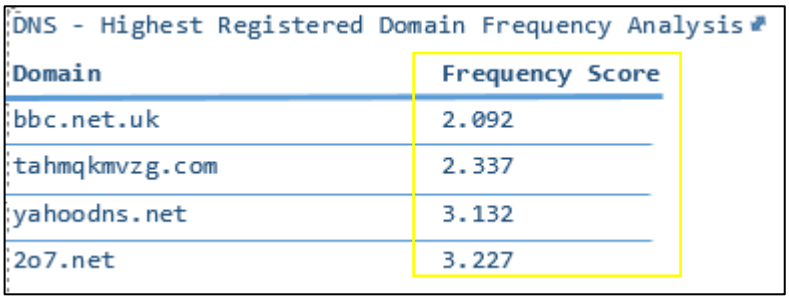
Componente de la suite ELK que permite la gestión de los índices a través del mantenimiento programado.

1.8.5.2 ElastAlert

Componente que permite realizar consultas en Elasticsearch y alerta sobre el comportamiento anómalo definido por el usuario.

1.8.5.3 FreqServer

Tal como se muestra en la figura 19-1, es una aplicación Web que trabaja de forma multiproceso, sirve para consultar y tabular tablas de frecuencia, por ejemplo, un conteo de las páginas más visitadas, el número de conexiones SSH activas o rehusadas, nombres de procesos y servicios, etc.



DNS - Highest Registered Domain Frequency Analysis

Domain	Frequency Score
bbc.net.uk	2.092
tahmqkmvzg.com	2.337
yahoodns.net	3.132
2o7.net	3.227

Figura 19-1: Frecuencia de consultas a los principales DNS registrados
Fuente: https://github.com/Security-Onion-Solutions/security-onion/wiki/FreqServer

1.8.5.4 DomainStats

De acuerdo con la figura 20-1, DomainStats es un componente de ELK capaz de obtener información adicional sobre un dominio, como el tiempo de creación, edad, reputación, etc. (Burks, 2017, https://github.com/Security-Onion-Solutions/security-onion/wiki)

DNS – Baby Domain Requests

Domain	Frequency Score	Count
adminaoffline.com	August 25th 2017, 12:41:24:000	3

Figura 20-1: Fecha de creación del Dominio
Fuente: https://github.com/Security-Onion-Solutions/security-onion/wiki/domainstats

1.9. Determinación del tipo y arquitectura de solución SIEM

En base a sus aplicativos funcionales, características de los fabricantes, licencias que gobiernan el producto, proveedores de soluciones SIEM y la comparativa entre SIEMs Comerciales tanto como Open Source, ha hecho que GARTNER haya publicado recientemente su Magic Quadrant (MQ) 2017 para información de seguridad y gestión de eventos (SIEM),

De acuerdo al gráfico 1-1 se muestra la comparativa realizada por GARTNER vigente a Diciembre de 2017.

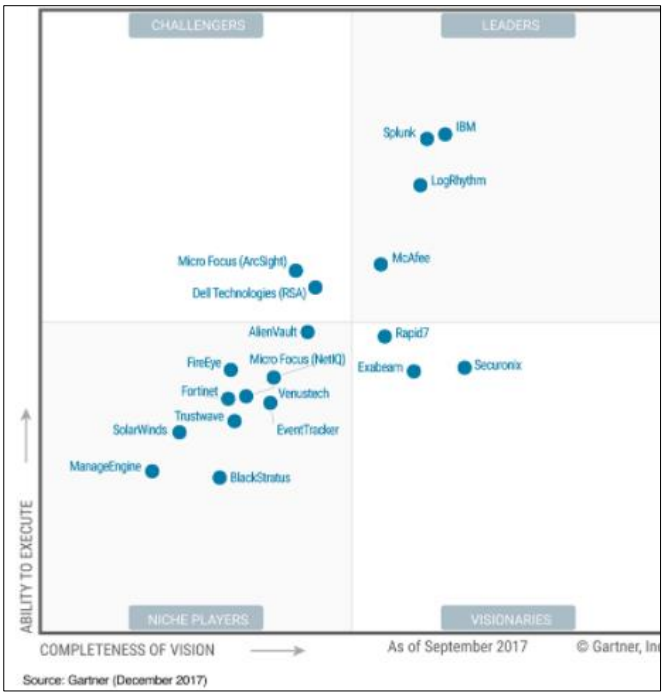


Gráfico 1-1: Cuadrante Mágico de Gartner para Soluciones SIEM a Diciembre 2017
Fuente: Gartner, 2017

En la tabla 2-1, se ha realizado una comparativa entre tres SIEMs opensource, analizando las características y funcionalidad, con el fin de encontrar una solución que cumpla con los requisitos planteados anteriormente.

Tabla 2-1: Comparativa SIEMs opensource

FABRICANTE /FUNCIONALIDAD	OSSIM	ALIENVAULT	SECURITY ONION
Tipo de Licencia	LGPL	Comercial - GPL	GPL
Interfaz Web	SI	SI	SI
Almacenamiento de Logs	SI	SI	SI
Correlación de Logs	SI	SI	SI
Gestión de Incidentes	SI	SI	SI
Módulo de Reportería	SI Limitado	SI	SI
Sistema IDS incluido	SI Snort	SI Snort	SI Snort/Suricata
Arquitectura modular y escalable	NO	SI	SI
Sistema de administración multiusuario	NO	SI	SI
Analizador de Vulnerabilidades	SI OpenVAS	SI OpenVAS	SI
Monitor de tráfico de Red	SI Ntop	SI Ntop	SI Sguil, Squert
Host IDS	SI Osiris	SI Osiris	SI Ossec
Sistema Antivirus incorporado	ClamAV	ClamAV	NO

Realizado por: Pazmiño, J; Pazmiño, C. 2018
Fuente: (Pazmiño Gómez, 2017)

Si bien todas las soluciones cumplen con el requisito de almacenamiento, correlación, gestión y módulos de reportería, únicamente OSSIM, ALIENVAULT y SECURITY-ONION recopilan un gran número de aplicativos destinados al análisis forense, tanto de redes como de sistemas, de manera que se pueda garantizar el correcto funcionamiento de los componentes y la inexistencia de todo tipo de intrusos en la red.

SECURITY ONION posee una gran variedad de paquetes y herramientas por defecto, para auditar la seguridad de todo tipo de redes, monitores de tráfico de red que permiten determinar el nivel de congestión que sufren los dispositivos, sistemas host IDS con el fin de determinar si una amenaza logro saltar la protección de los dispositivos de seguridad perimetral y se encuentra a punto de ejecutar código en las pc de los usuarios finales, como características particulares de SECURITY ONION se puede citar:

- GPL - Licencia Pública General.
- Modelos NSM (Network Security Monitor) adaptados para pequeñas, medianas y grandes compañías.
- No tiene límite para integrar dispositivos.
- Sin coste adicional por las funcionalidades de seguridad incorporadas (NIDS, HIDS, WIDS, Administración de las vulnerabilidades, Monitorización de Red, etc.)
- De ser necesario integrar nuevos conectores no tiene restricciones
- Suite opensource de poderosas herramientas de tráfico
- Solución unificada de un SIEM con muchas otras funcionalidades de seguridad.
- Integración con sistemas informáticos y herramientas multiplataforma.
- Personalización de cuadro de mandos e informes a la imagen corporativa.
- Escalabilidad, dónde no existe un límite en crecimiento de la plataforma.
- Adaptabilidad que permite activar/desactivar las funcionalidades basado en las necesidades del proyecto.

De acuerdo al análisis mostrado, y teniendo en cuenta el beneficio de las soluciones analizadas, para el desarrollo de la presente se utilizará la versión 14.04.5.4 de Security Onion.

CAPÍTULO II

2. IMPLEMENTACIÓN DE LA INVESTIGACIÓN

2.1. Análisis de la Infraestructura de red

Para establecer el diseño de la solución propuesta, se solicitó la topología actual de la red corporativa de la "EERSA" la misma que fue proporcionada por la Ing. Andrea Vallejo que cumple con la función de "Administrador de Red".

En la figura 1-2, se muestra la Topología de Red Corporativa "EERSA" en la actualidad.

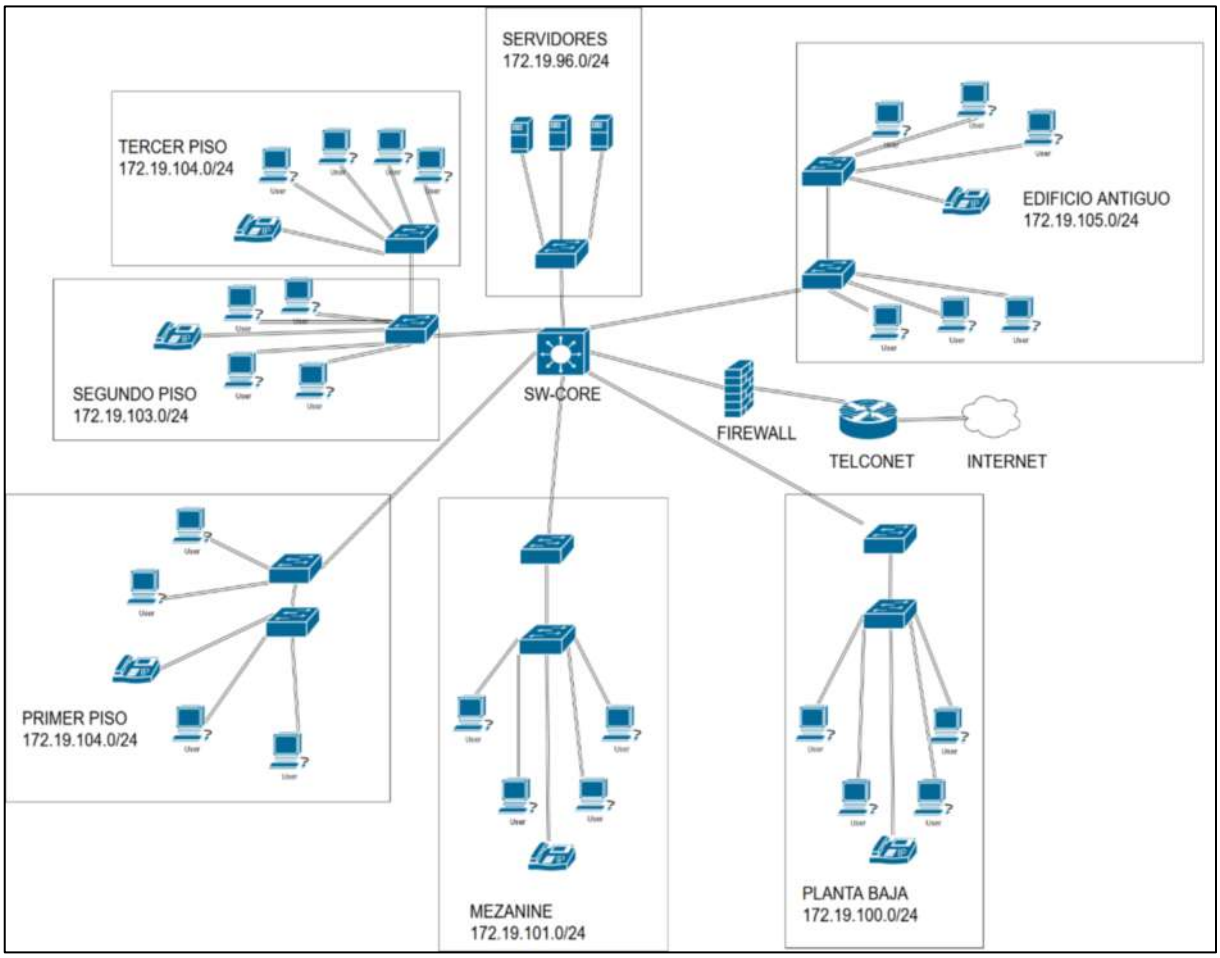


Figura 1-2: Topología de Red Corporativa "EERSA" en la actualidad
Realizado por: EERSA, 2018

Una vez analizada y estudiada la topología de red de la "EERSA", se implementó el correlacionador de eventos SECURITY ONION respecto a otras opciones, debido a que este, posee una gran variedad de paquetes y herramientas opensource por defecto, una mayor capacidad para auditar la seguridad de todo tipo de redes, licencia totalmente GPL y entre una característica superior de las otras, la integración de Elastic Stack en el Kernel.

Para el servidor, respecto a Hardware, es necesario que cuente con 2 interfaces de red, la primera para la administración y monitoreo del correlacionador mediante el uso de la suite TCP/IP, y la segunda para el análisis del tráfico de red en modo SPAN.

SECURITY ONION posee una gran variedad de paquetes y herramientas por defecto, para auditar la seguridad de todo tipo de redes, monitores de tráfico de red que permiten determinar el nivel de congestión que sufren los dispositivos, sistemas host IDS con el fin de determinar si una amenaza logro saltar la protección de los dispositivos de seguridad perimetral y se encuentra a punto de ejecutar código en las pc de los usuarios finales, como características particulares de SECURITY ONION se puede citar:

En los dispositivos de red tales como switches y routers se configuró el protocolo de envío de mensajes SYSLOG, que funciona mediante la topología cliente-servidor siendo el servidor el correlacionador de eventos implementado.

Para el monitoreo de servidores se configuró el sistema de detección de intrusos OSSEC, que al igual que SYSLOG funciona a través de topología cliente-servidor.

2.2. Diseño de la arquitectura propuesta

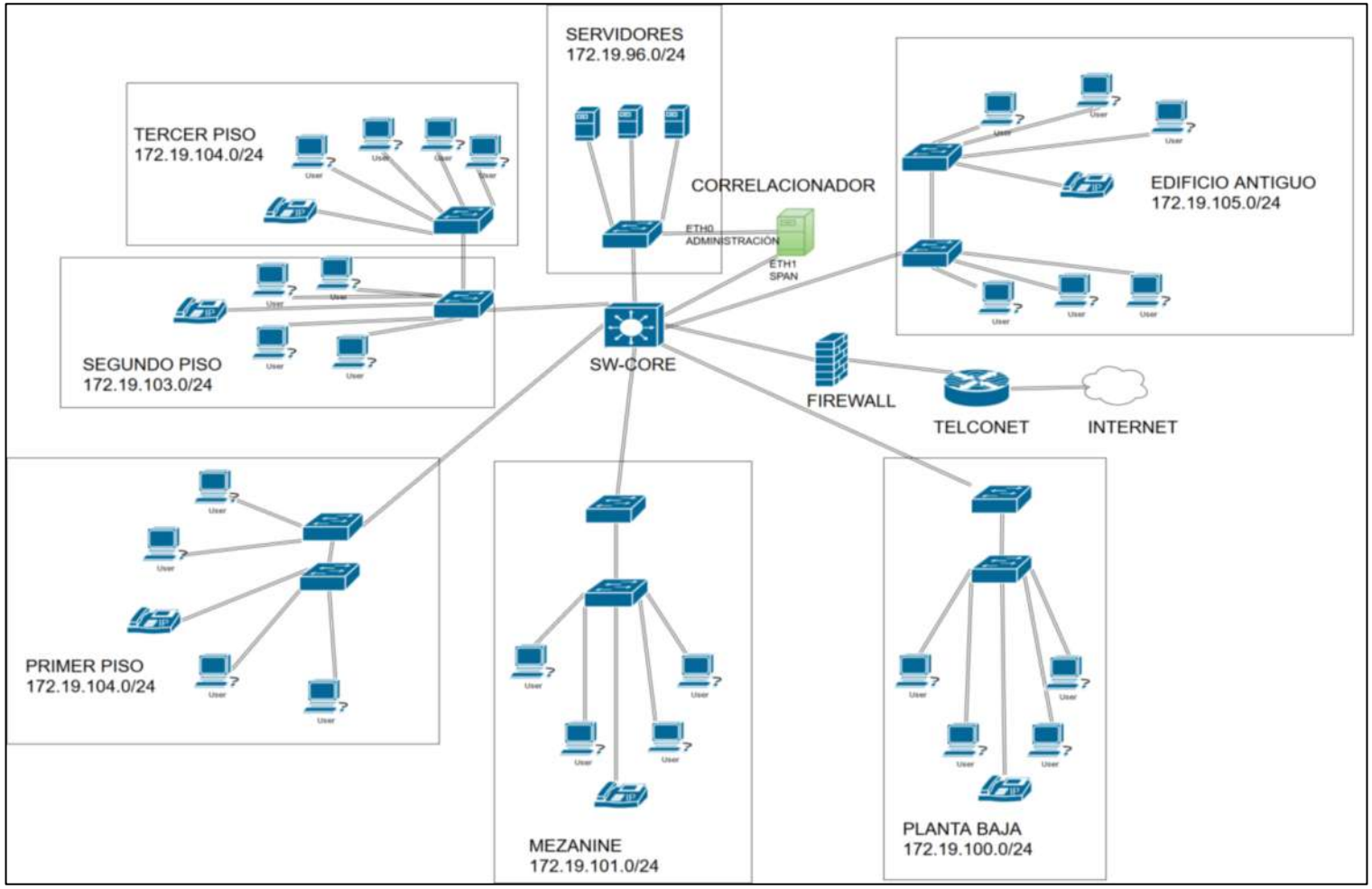


Figura 2-2: Solución propuesta, para la implementación del SIEM
Realizado por: Pazmiño, J; Pazmiño, C. 2018

2.3. Implementación de la tecnología

2.3.1 Instalación cliente y servidor

2.3.1.1 Requisitos técnicos para la implementación del servidor Security Onion

Los requisitos de hardware para instalar la versión 14.04.5.4 de Security Onion dependerán 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, y de la cantidad de hosts disponibles en la red que pretendamos analizar: *https://github.com/Security-Onion-Solutions/security-onion/wiki/Hardware*

- *Servidor principal*

El servidor principal debe tener de 1 a 4 núcleos de CPU, de 8 a 16 GB de RAM y de 100 GB a 1 TB de espacio en disco. También es factible la utilización de máquinas virtuales, ya que tiene requisitos de hardware más bajos que los sensores, pero necesita una mayor fiabilidad y disponibilidad.

- *Sensores*

Los siguientes requisitos de hardware se aplican a los sensores. No se aplican a instalaciones exclusivas como se describió previamente.

- *Virtualización*

De acuerdo a la documentación oficial del fabricante, se recomienda la implementación de la solución sobre hardware físico dedicado (especialmente el sistema estará en producción) esto a fin de evitar competir por los recursos de CPU, RAM y RED con otras soluciones virtualizadas en el mismo host. Los sensores se pueden virtualizar, pero deberá tener en cuenta las recomendaciones de asignación física previamente indicadas.

➢ *MEMORIA RAM*

El uso de RAM depende en gran medida de los siguientes factores:

- El número de servicios que vamos a habilitar en el correlacionador de eventos.
- El tipo de tráfico a monitorear
- La cantidad real de tráfico que está monitoreando (ejemplo: puede estar monitoreando un enlace de 1Gbps pero solo está usando 200Mbps la mayor parte del tiempo)
- La cantidad de pérdida de paquetes que es "aceptable" para la organización
- Las siguientes estimaciones de memoria RAM son una guía aproximada y se supone que va a ejecutar Snort/Suricata, Bro y netsniff-ng (captura de paquetes completos) y desea minimizar o de ser posible eliminar la pérdida de paquetes.

NOTA: Los valores requeridos en RAM son una referencia mínima para su funcionamiento, pero es importante mencionar que a mayor cantidad de memoria RAM, será mejor su funcionamiento.

En la tabla 1-2, se muestra los requerimientos mínimos de RAM para un funcionamiento correcto del SIEM.

Tabla 1-2: Requerimientos mínimos de RAM para el funcionamiento del SIEM.

TIPO DE IMPLEMENTACIÓN	CANTIDAD DE TRÁFICO	REQUERIMIENTO EN RAM
Virtualización - Prueba	20 Mbps o menos	Min:3 GB
Física – Red Pequeña Producción	50 Mbps o menos	Min:8 GB
Física – Red Mediana Producción	50 Mbps – 500 Mbps	Min:16GB - 128GB
Física – Red Grande Producción	500 Mbps - 1000 Mbps	Min:128GB - 256GB

Fuente: (Security Onion Solutions, 2017)

➢ *Almacenamiento*

Los sensores que tienen habilitada la opción de captura completa de paquetes, necesitan una gran cantidad de espacio de almacenamiento. Por ejemplo, supongamos que se está monitoreando un

enlace que promedia 50Mbps, entonces 50Mb / s = 6.25 MB / s = 375 MB / minuto = 22,500 MB / hora = 540,000 MB / día. Por lo tanto, necesitará unos 540 GB para los archivos pcaps de un día (se debe multiplicar esto por la cantidad de días que desee conservar en el disco para fines forenses o de investigación). Se debe tener en cuenta que esto es solo pcaps y Elactic Stack también necesitará espacio en el disco. De forma predeterminada, la configuración por defecto del parámetro log_size_limit de Elastic Stack es de aproximadamente el 50% del espacio en disco dejando aproximadamente la otra mitad del disco para la captura completa de paquetes. Cuanto más espacio en disco tenga, más retención de registros tendrá. (Burks, 2017, https://github.com/Security-Onion-Solutions/security-onion/wiki)

2.4. Implementación

Para la Red Interna de la Empresa Electrica "Riobamba S.A", se estima un nivel de tráfico de alrededor de 20MBps, para lo cual se propone, un requerimiento mínimo de 8GB en RAM, y para el disco duro 140 GB, de acuerdo con la cantidad de logs que se va a almacenar y el tiempo que van a permanecer en el Correlacionador de Eventos

Se implementa la tecnología utilizando los equipos físicos de la EERSA en un entorno de producción. Las características de los equipos se describen a continuación.

2.4.1 Topología de la Red

En la siguiente tabla 2-2, se ha realizado una descripción de Hardware y Software, de los dispositivos que forman parte de la Topología de Red Corporativa de la "EERSA".

Tabla 2-2: Descripción de Hardware y Software, en la Topología de Red Corporativa"EERSA"

Descripción	Conexión de Red	Características	IP
Servidor Security Onion	Red Interna (RED SERVIDORES) LAN	Server HP ProLiant DL380 G5 • Dual Core a 2,83 GHz • 4GB RAM – 140 HD • 2 interfaces físicas	xx.yy.zz.50/24
Switch de Core	Red Interna (RED SERVIDORES) LAN	Cisco Catalyst 4507R • 48 Gbps/slot, 7 SLots • Hasta 240 puertos 10/100/1000BASE-T Gigabit Ethernet	xx.yy.zz.1/24 vlan1

Servidor DNS	Red Interna (RED SERVIDORES) LAN	HP ProLiant DL380 G5 • Sistema Operativo Centos 6	xx.yy.zz.7/24
Servidor Correo – Zimbra	Red Interna (RED SERVIDORES) LAN	HP ProLiant DL380 G5 • Sistema Operativo Centos 6	xx.yy.zz.252/24
Servidor Facturación	Red Interna (RED SERVIDORES) LAN	HP Compaq Pro 6300 Microtower • Sistema Operativo Centos 6	xx.yy.zz.21/24
Servidor Cocinas de Inducción	Red Interna (RED SERVIDORES) LAN	HP Compaq Pro 6300 Microtower • Sistema Operativo Centos 6	xx.yy.zz.20/24
Equipo de Analista	LAN	Windows XP	xx.yy.zz.14/25

Realizado por: Pazmiño, J; Pazmiño, C. 2018

Para la implementación del Servidor Security Onion, se utilizará la versión 14.04.5.4, disponible en, la siguiente dirección:
https://github.com/Security-Onion-Solutions/securityonion/releases/tag/v14.04.5.4_20171031
Para la implementación se requiere 2 interfaces físicas, las cuales estarán configuradas de la manera que se muestra en la tabla 3-2, por motivos de confidencialidad no se puede especificar la dirección ip.

Tabla 3-2: Descripción y direccionamiento IP de las Interfaces.

INTERFÁZ	Descripción	Direccionamiento
Eth0	Interfaz de administración (preferiblemente conectada a una red de administración dedicada) usando DHCP o preferiblemente IP estática	IP Estática: xx.yy.zz.50/24
Eth1	Interfaz de "escucha" o modo promiscuo (sin dirección IP). En esta interfaz se configura SPAN(Switch Port Analizer) + Port Mirroring, con la finalidad de clonar la interfaz física de salida a la WAN y capturar la mayor cantidad de tráfico.	Sin dirección IP

Realizado por: Pazmiño, J; Pazmiño, C. 2018

2.4.2 Instalación de Security Onion

En la figura 3-2, se muestra el Switch de Core actual, Cisco Catalyst 4507R, que forma parte de la infraestructura de la Dirección de Computo de la EERSA.

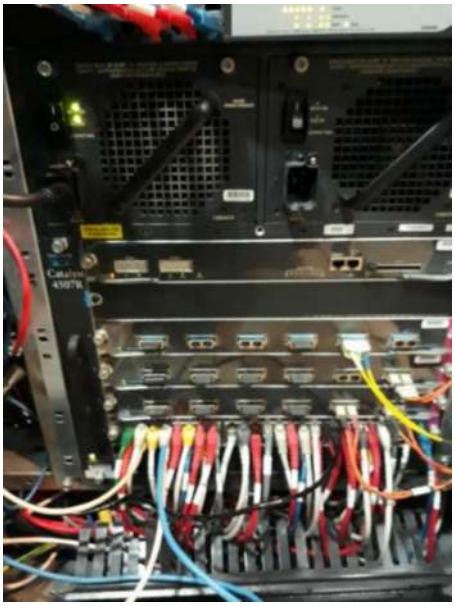


Figura 3-2: Fotografía del Switch de Core Cisco Catalyst 4507R - EERSA
Realizado por: Pazmiño, J; Pazmiño, C. 2018

En la figura 4-2, se muestra la conexión de la interfaz eth0 proveniente del correlacionador de eventos, y directamente conectada al Switch de Core, a través de la Interfaz Gigabit Ethernet 0/7.

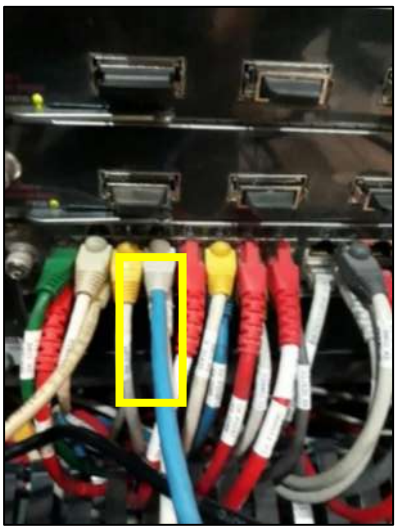


Figura 4-2: Interfaz de administración,
conectada al Switch de Core en Fast Ethernet 0/7
Realizado por: Pazmiño, J; Pazmiño, C. 2018

En la figura 5-2, se muestra las características físicas del servidor proporcionado por la Dirección de Computo de la Empresa Eléctrica “Riobamba S.A”.

- MODELO: Server HP ProLiant DL380 G5

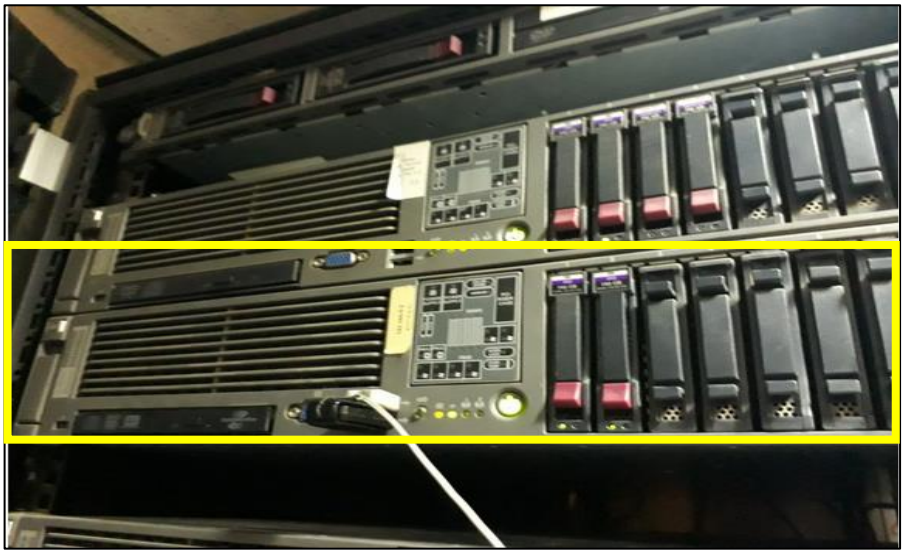


Figura 5-2: Fotografía Server HP ProLiant DL380 G5
Realizado por: Pazmiño, J; Pazmiño, C. 2018

En la figura 6-2, se muestra las características de procesamiento y memoria del servidor HP ProLiant DL380 G5.

- CPU: 4 núcleos
- RAM: 4 GB
- DISCO DURO: 150 GB

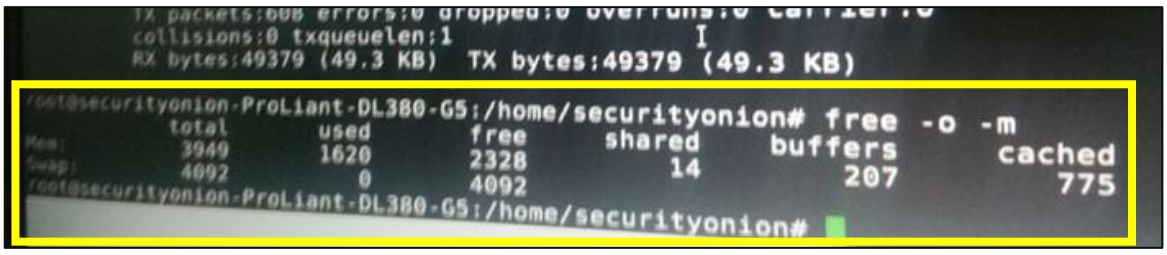


Figura 6-2: Características de procesamiento y memoria del servidor HP ProLiant DL380 G5
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Posteriormente, al haber tomado en cuenta los recursos para la implementación, procedemos con la Instalación. Encendemos el servidor HP Proliant e ingresamos a la BIOS, con la finalidad de arrancar desde una unidad extraíble, en este caso utilizaremos un DVD con la imagen iso de SecurityOnion versión 14.04.5.4 de 64 bits. Reiniciamos el servidor y podemos ver la pantalla de instalación del SIEM, como se muestra en la figura 7-2. La primera pantalla nos muestra el idioma de instalación, especificamos el idioma de preferencia y continuamos el proceso:

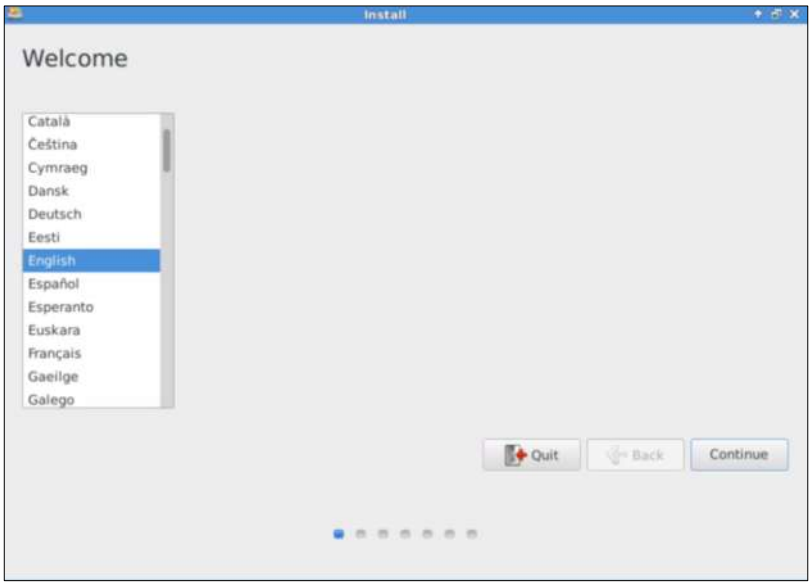


Figura 7-2: Idioma de Instalación
Realizado por: Pazmiño, J; Pazmiño, C. 2018

En la figura 8-2, se muestra el asistente de instalación, el cual verifica las características y requerimientos mínimos para un correcto funcionamiento.

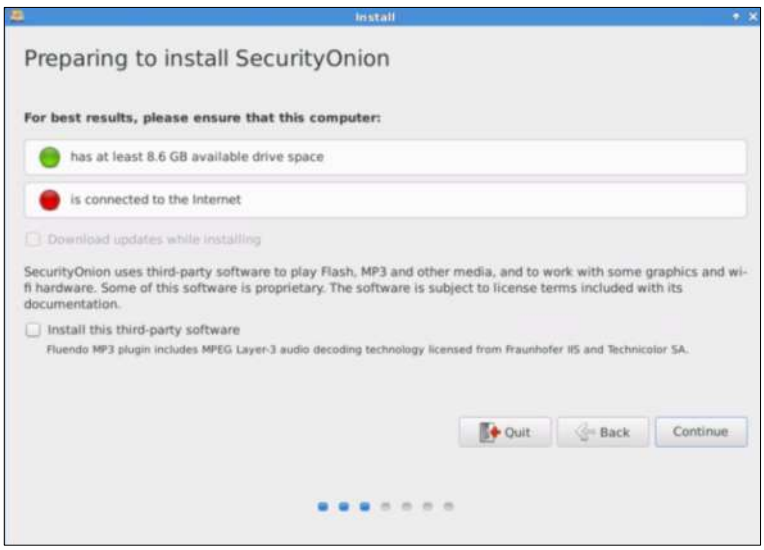


Figura 8-2: Características y Requerimientos de Instalación
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Como se muestra en la figura 9-2, se debe especificar el tipo y tamaño de partición que utilizará la solución propuesta, teniendo en cuenta que se recomienda utilizar la totalidad del disco duro asignado para la recolección y procesamiento de datos. En ambientes de producción con gran afluencia de información se puede generar un arreglo de discos mediante LVM.

Figura 9-2: Tipo de Instalación
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Se validan las configuraciones especificadas previo el inicio de la instalación, de tal manera como se muestra en la figura 10-2.

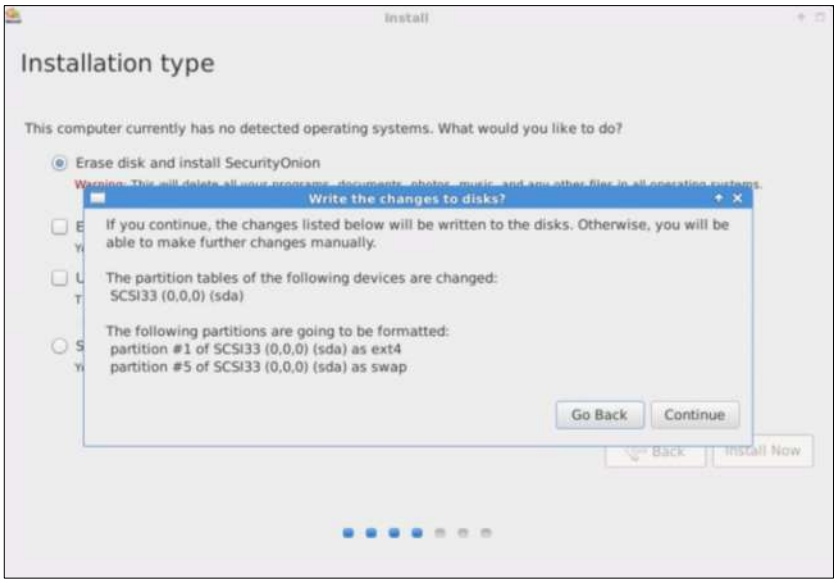


Figura 10-2: Tamaño de Partición de Memoria
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Es necesario especificar la zona horaria que utilizará el sensor, para esta instalación se recomienda Guayaquil – Ecuador (GMT -5). Es necesario especificar en los demás servidores de infraestructura la misma zona horaria, así como la gestión y sincronización de las horas mediante el uso de NTP, como se muestra en la figura 11-2.

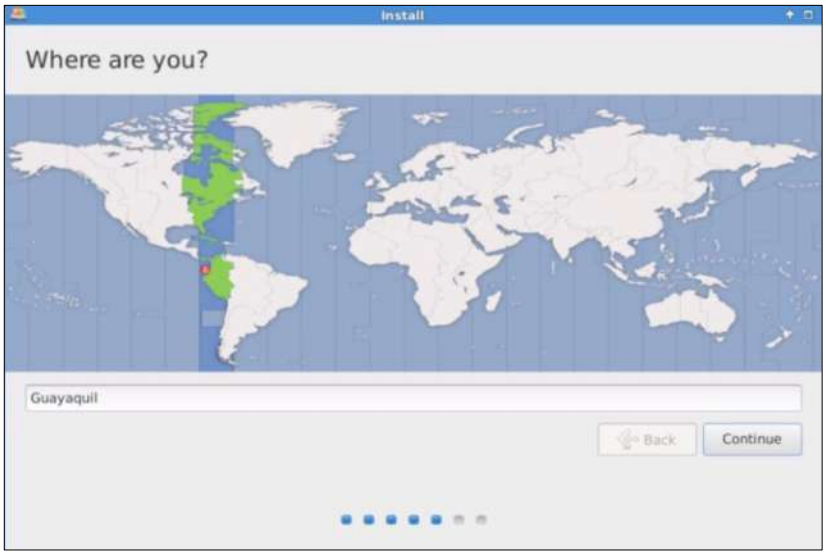


Figura 11-2: Selección de Zona Horaria (GMT-5)
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Seleccionamos el idioma e ingreso de teclado, en este caso modelo Español (Latino Americano) e idioma Español (Latino), como se muestra en la figura 12-2.

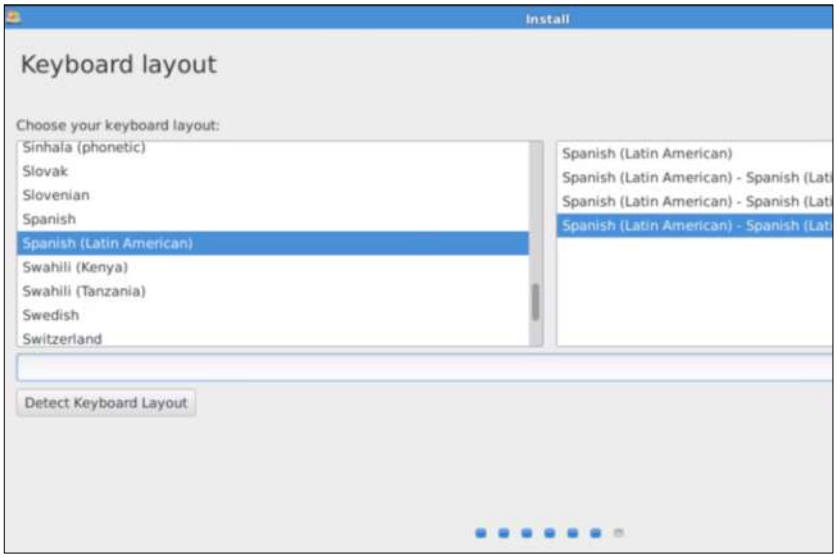


Figura 12-2: Idioma e Ingreso del Teclado
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Como se muestra en la figura 13-2, llenamos los campos de instalación solicitados con el Nombre de Usuario, y una contraseña.
Username:securityonion

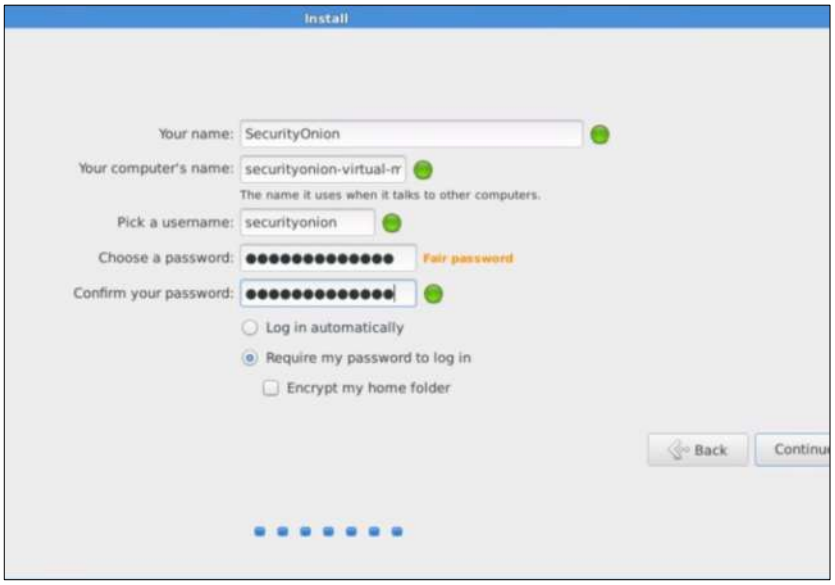


Figura 13-2: Registro de Usuario y Contraseña
Realizado por: Pazmiño, J; Pazmiño, C. 2018

La instalación de Security Onion, se realiza correctamente y se descomprime el sistema operativo, se copian los archivos de instalación y se ejecutan en el servidor, como se muestra en la figura 14-2.

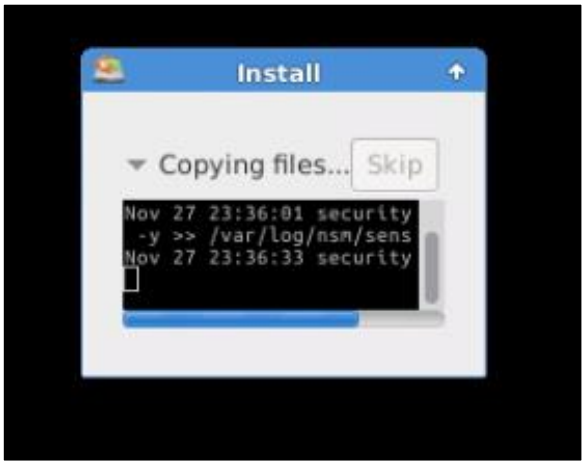


Figura 14-2: Copiado e Instalación de archivos
Realizado por: Pazmiño, J; Pazmiño, C. 2018

De tal manera, como nos muestra la figura 15-2, la instalación ha finalizado con éxito, reiniciamos el servidor para comprobar.

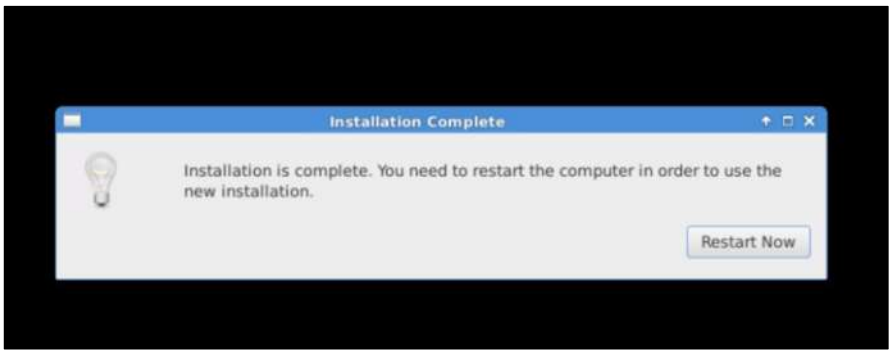


Figura 15-2: Instalación Completada
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Al reiniciar el servidor nos aparece el GNU Grub de Security Onion, y seleccionamos la distribución instalada, como se muestra en la figura 16-2

Figura 16-2: GNU Grub de Security Onion
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Como se muestra en la figura 17-2, ingresamos las credenciales de autenticación y accedemos al SIEM.

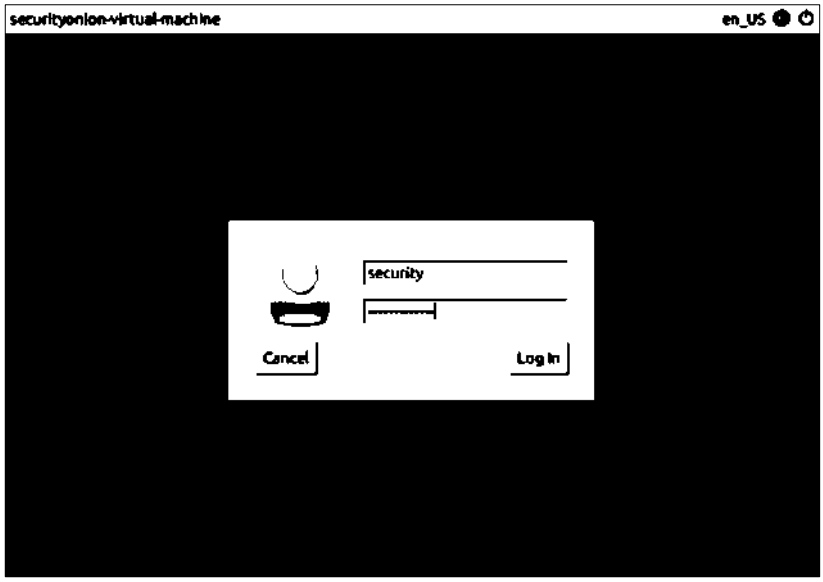


Figura 17-2: Ingreso de Credenciales
Realizado por: Pazmiño, J; Pazmiño, C. 2018

De acuerdo a la figura 18-2, se muestra instalado de manera correcta, el Sistema Operativo Security Onion 14.04.5.4. El cual nos servirá como base para la implementación de todos los sistemas de almacenamiento de logs, detección de instrusos y herramientas para la correlación de eventos, propuestos anteriormente.

Figura 18-2: Security Onion
Realizado por: Pazmiño, J; Pazmiño, C. 2018

La figura 19-2, muestra una fotografía, de la tecnología implementada en el servidor HP ProLiant DL380 G5.

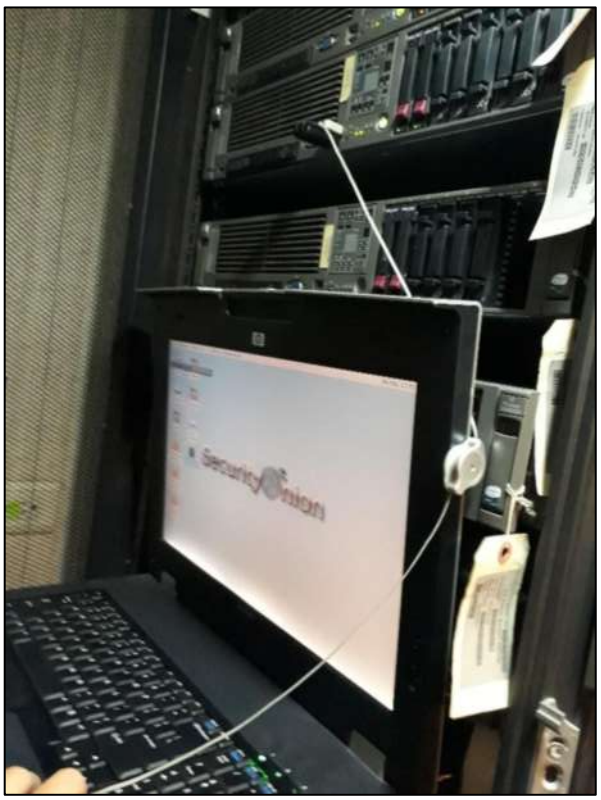


Figura 19-2: Fotografía de Instalación completada – Security Onion
Realizado por: Pazmiño, J; Pazmiño, C. 2018

2.4.3 Configuración de Interfaces, y de las herramientas de Análisis.

A continuación, vamos a configurar las interfaces, y sus principales herramientas de análisis tales como Kibana, Snort, ElasticSearch, etc. De tal manera, como se muestra en la figura 20-2.

Figura 20-2: Wizard para la configuración de Interfaces
Realizado por: Pazmiño, J; Pazmiño, C. 2018

El wizard de configuración nos pregunta si deseamos configurar las interfaces en este momento. Aceptamos y continuamos con la instalación. De tal manera, como se muestra en la figura 21-2.

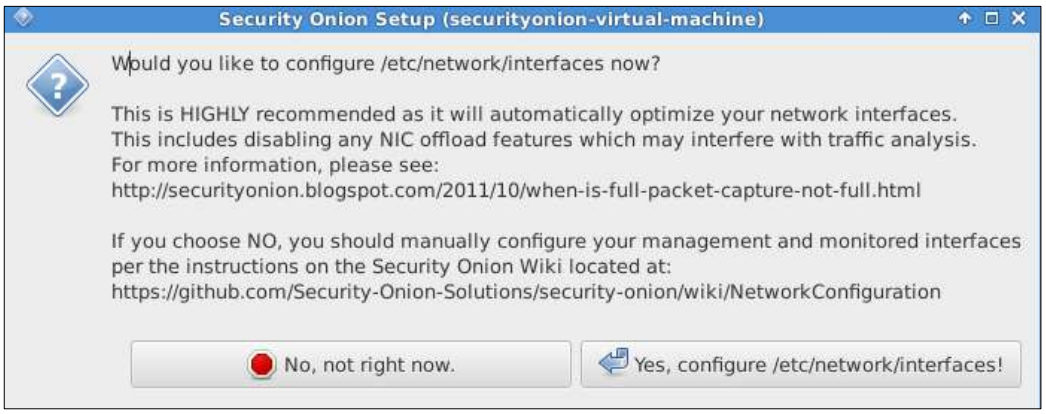


Figura 21-2: Configuración de Interfaces
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Como indica, la figura 22-2, se debe especificar la interfaz de red que se establecerá para la administración de la plataforma. Para este caso utilizaremos la interfaz eth0.

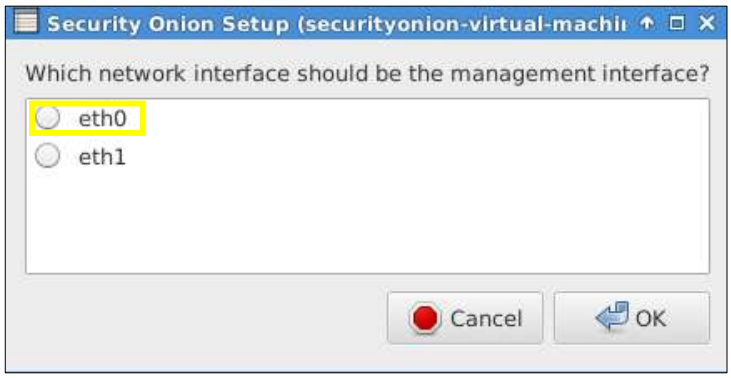


Figura 22-2: Interfaz de Administración - eth0
Realizado por: Pazmiño, J; Pazmiño, C. 2018

De tal manera, como se muestra en las figuras 23-2 y 24-2. Ingresamos la dirección IP estática: xx.yy.zz.50 y máscara /24, dirección IP de administración del servidor "Security Onion", proporcionada por la Ing. Andrea Vallejo – Administradora de Red de la EERSA.

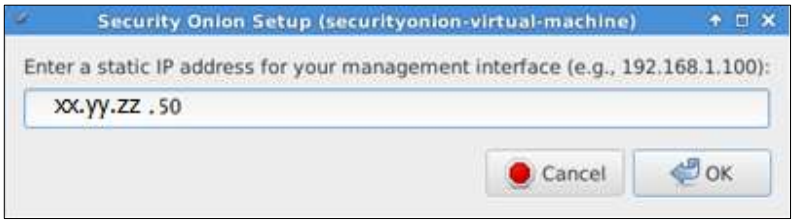


Figura 23-2: Dirección IP para la administración del Correlacionador de Eventos
Realizado por: Pazmiño, J; Pazmiño, C. 2018

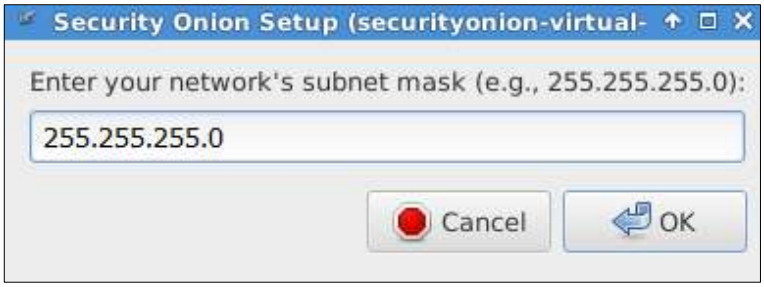


Figura 24-2: Máscara de Red para el Correlacionador de Eventos
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Asignamos la dirección IP de salida al Gateway: xx.yy.zz.1; dirección IP para el servicio de DNS:xx.yy.zz.7 ; y el nombre del dominio local: "eersa.com.ec", como se muestra en la figura 25-2.

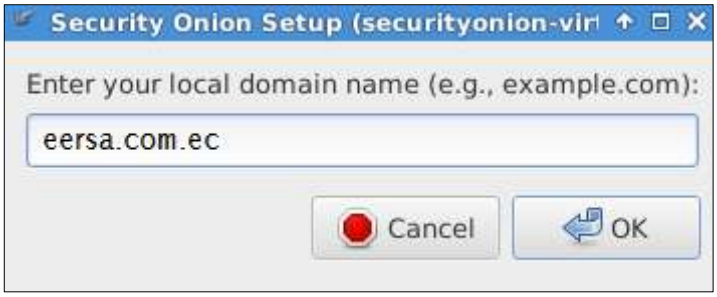


Figura 25-2: Dominio local
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Como indica la figura 26-2, tenemos la opción de configurar la interfaz de monitoreo. Aceptamos y continuamos.

Figura 26-2: Configuración de interfaz de monitoreo
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Seleccionamos la interfaz que será utilizada para monitoreo, en este caso "eth1", como se muestra en la figura 27-2.

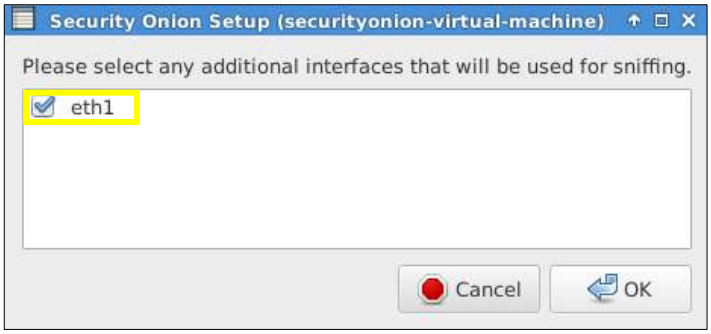


Figura 27-2: Interfaz de monitoreo
Realizado por: Pazmiño, J; Pazmiño, C. 2018

De acuerdo con la figura 28-2, se muestra un resúmen de las direcciones ip asignadas, interfaces administración - monitoreo, y dominios de DNS configurados.

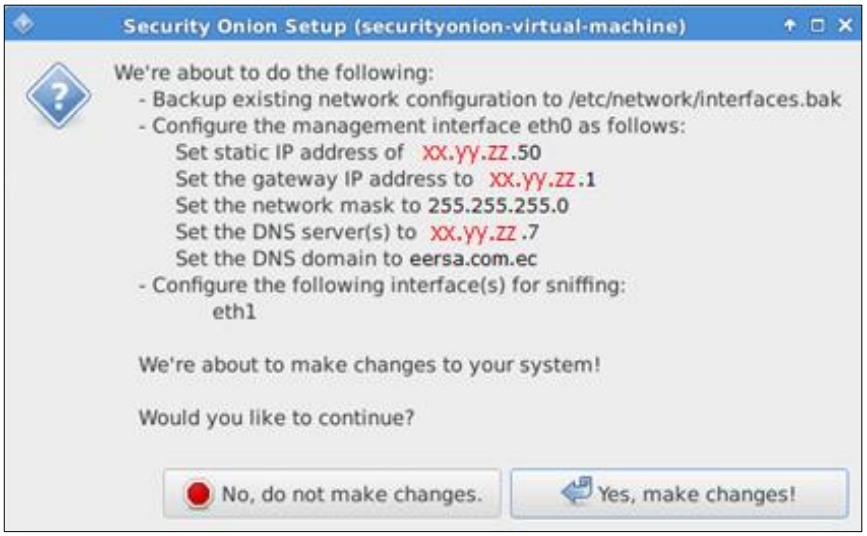


Figura 28-2: Resúmen de Direccionamiento y configuración de Interfaces.
Realizado por: Pazmiño, J; Pazmiño, C. 2018

La configuración de red ha sido completada con éxito, de acuerdo a la figura 28-2, nos indica la ruta del archivo para la configuración de red, en caso de ser necesario, realizar cualquier cambio manualmente en */etc/network/interfaces* y se deberá reiniciar el servidor para aplicar todos los cambios.

Una vez reiniciado el servidor, y de acuerdo a la figura 29-2, se deberá especificar el tipo de arquitectura que será implementada en la presente instalación teniendo en cuenta sus características, las cuales son:

- **Servidor**: en este modo, se instalan únicamente herramientas que permiten visualizar y procesar datos provenientes de otras implementaciones de Security Onion.

- **Sensor:** este será el modo que recolectará datos y los enviará para el procesamiento de la solución si se lo establece en modo Server.

- **Standalone** cumple con las funciones de Server y Sensor simultáneamente, su administración puede ser desde la misma máquina, o desde una conexión a través de SSH.

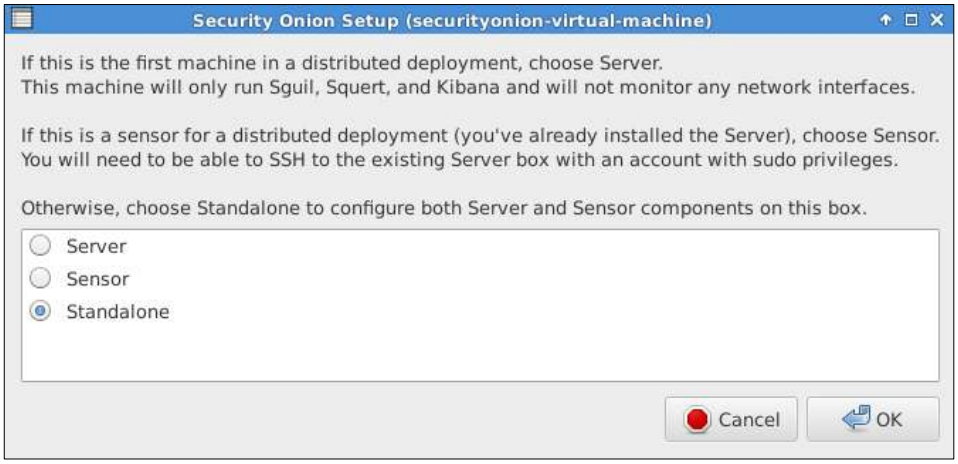


Figura 29-2: Especificación del tipo de Arquitectura
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Se deberá especificar las credenciales administrativas, las cuales permitirán interactuar con las herramientas de monitoreo y gestión, como indica la figura 30-2.

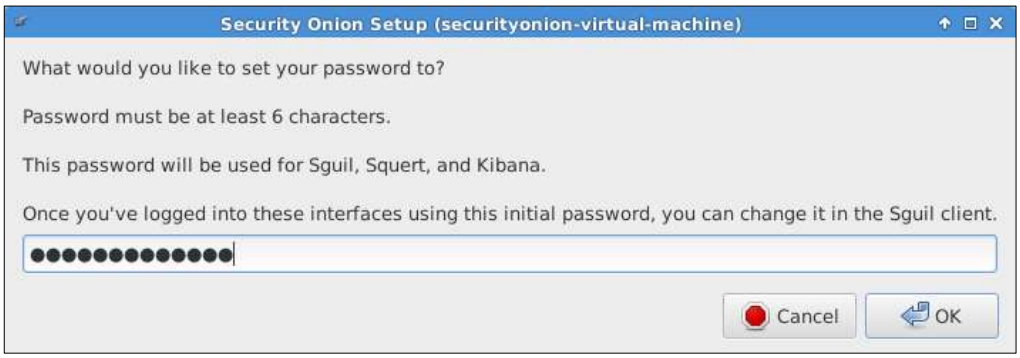


Figura 30-2: Ingreso de credenciales
Realizado por: Pazmiño, J; Pazmiño, C. 2018

De acuerdo con la figura 31-2, se debe especificar el número de conexiones de PF_RING.Este valor depende de la capacidad de procesamiento del servidor. Para el presente utilizaremos un PF_RING de 14 con la finalidad de aumentar las thread para el análisis de cada paquete, entonces 2^14=16384

Figura 31-2: Cálculo de PR_RING
Realizado por: Pazmiño, J; Pazmiño, C. 2018

De acuerdo con la figura 32-2, se muestra un resumen de las configuraciones que han sido previamente establecidas.

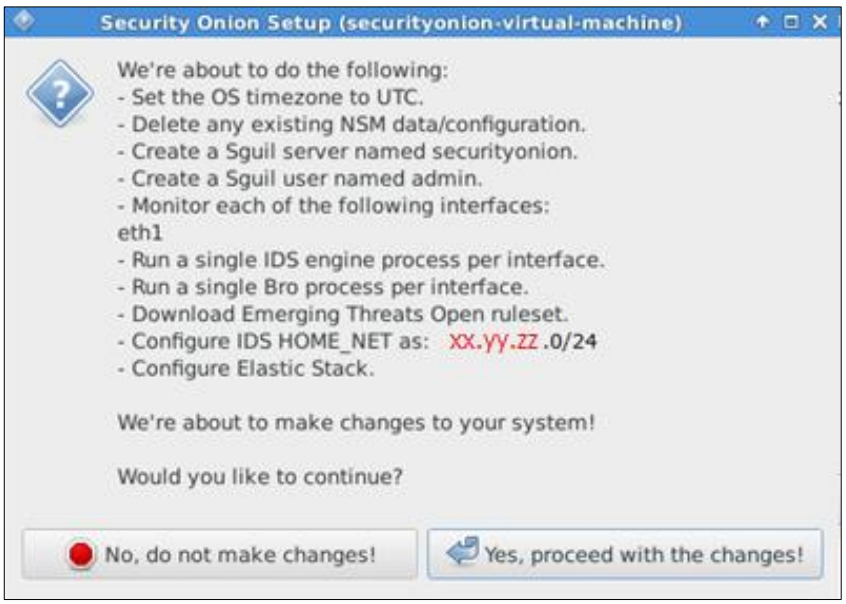


Figura 32-2: Resúmen de Configuraciones
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Las siguientes rutas, describen los archivos para eliminar, modificar o actualizar nuevas reglas para la herramienta NIDS Snort.

/etc/nsm/rules/downloaded.rules

/etc/nsm/rules/local.rules

/etc/nsm/pulledpork/

sudo rule-update

2.4.4 Configuración de OSSEC en los Servidores

Para el monitoreo de los servidores se instaló OSSEC en su versión 2.8.3 la misma que se la descargo de la siguiente dirección: https://dl.bintray.com/ossec/ossec-hids/ossec-hids-2.8.3.tar.gz, de tal manera como se muestra en la figura 33-2.

Figura 33-2: Descarga e instalación de paquetes OSSEC
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Como se muestra en la figura 34-2, se configura el idioma para el proceso de la instalación en este caso español por lo cual digitamos "es".

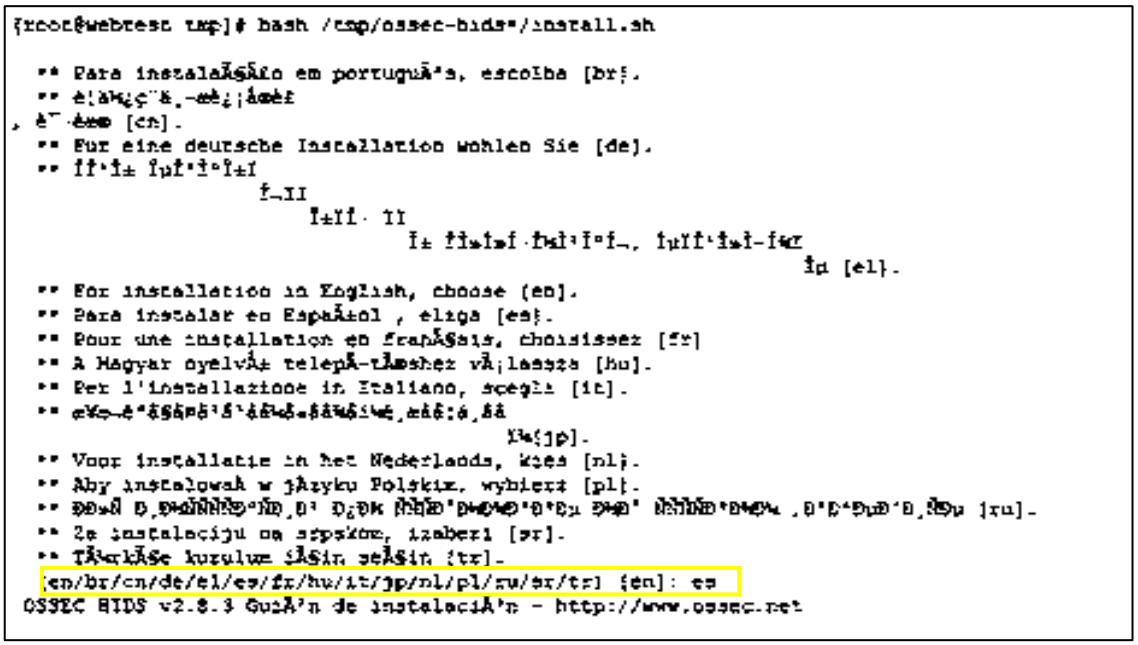


Figura 34-2: Selección de Idioma para el Servidor OSSEC
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Posteriormente, seleccionamos el tipo de instalación que vamos a realizar, como se mencionó antes utilizaremos la topología Cliente-Servidor por lo que procedemos a escribir la palabra "agente" con esto nuestro servidor enviará todos sus logs al correlacionador de eventos.

Luego nos muestra el directorio en donde se instalará OSSEC por defecto viene en el directorio /var/ossec/ pero si deseamos cambiarlo lo podemos realizar.

En este punto de la instalación nos pedirá que ingresemos la dirección ip de nuestro correlacionador de eventos la cual es: xx.yy.zz.50, como se muestra en la figura 35-2.

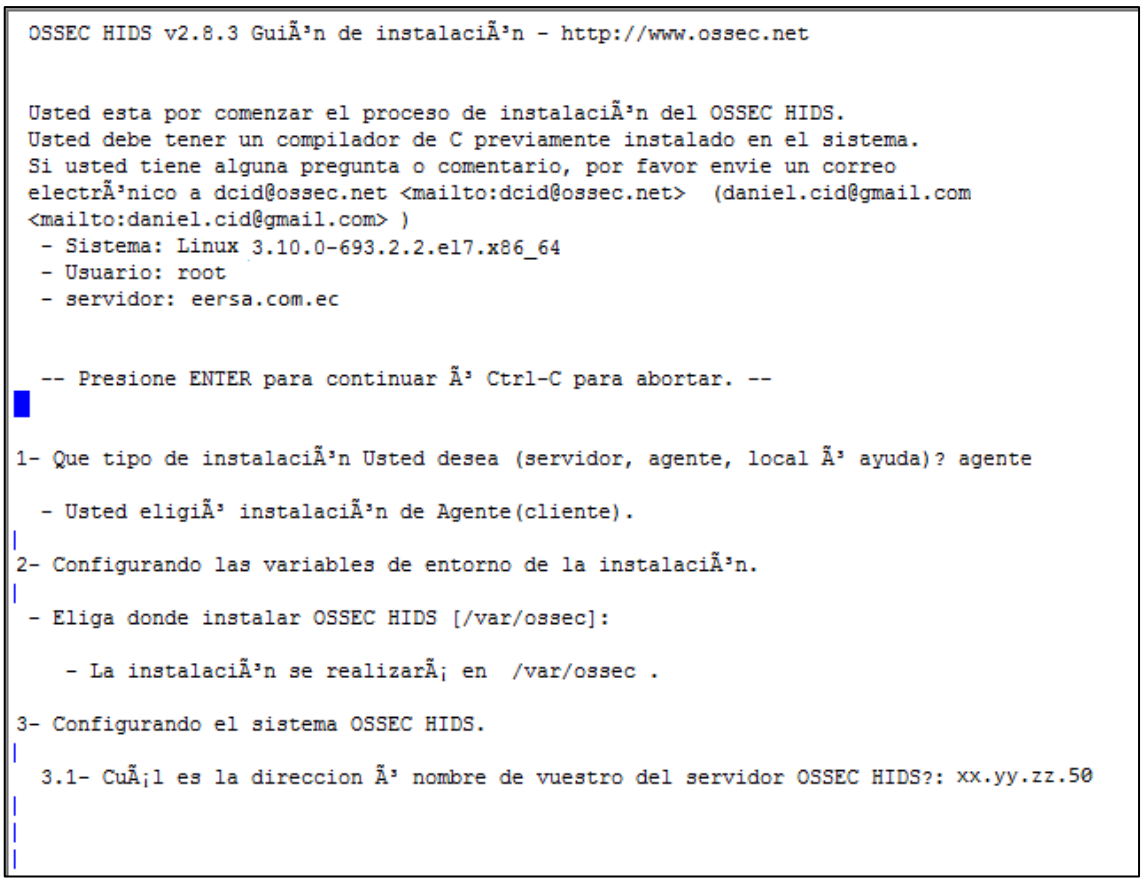


Figura 35-2: Configuración del Agente OSSEC
Realizado por: Pazmiño, J; Pazmiño, C. 2018

De acuerdo con la figura 36-2, habilitamos las opciones que nos sugiere la configuración, siendo:

- Syscheck: Se ejecuta periódicamente para comprobar si existen cambios en los archivos de configuración.
- Rootcheck: Su función es detectar la instalación o ejecución de posibles rootkits en el sistema

- Respuesta Activa: Medidas que tomará el agente ossec en caso de un ataque informático

```
3.2- Desea Usted agregar el servidor de integridad del sistema? (s/n) [s]:

 - Ejecutando syscheck (servidor de integridad del sistema).

3.3- Desea Usted agregar el sistema de detecciÃ³n de rootkit? (s/n) [s]:

 - Ejecutando rootcheck (sistema de detecciÃ³n de rootkit).

3.4 - Desea Usted habilitar respuesta activa? (s/n) [s]:
```

Figura 36-2: Opciones de Configuración
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Una vez hecho esto, la instalación del agente OSSEC habrá terminado, como se muestra en la figura 37-2.

```
make[1]: se ingresa al directorio `/tmp/ossec-hids-2.8.3/src/syscheckd'
cp -pr ossec-syscheckd ../../bin
make[1]: se sale del directorio `/tmp/ossec-hids-2.8.3/src/syscheckd'
make[1]: se ingresa al directorio `/tmp/ossec-hids-2.8.3/src/monitord'
cp -pr ossec-monitord ../../bin
cp -pr ossec-reportd ../../bin
make[1]: se sale del directorio `/tmp/ossec-hids-2.8.3/src/monitord'
make[1]: se ingresa al directorio `/tmp/ossec-hids-2.8.3/src/os_auth'
cp -pr ossec-authd ../../bin
cp -pr agent-auth ossec-authd ../../bin
make[1]: se sale del directorio `/tmp/ossec-hids-2.8.3/src/os_auth'
useradd: aviso: el directorio personal ya existe.
No se va a copiar ningÃºn fichero del directorio Â«skelÂ» en Ã©l.


 - El sistema es Redhat Linux.
 - Init script modificado para empezar OSSEC HIDS durante el arranque.

 - ConfiguraciÃ³n finalizada correctamente.

 - Para comenzar OSSEC HIDS:
              /var/ossec/bin/ossec-control start

 - Para detener OSSEC HIDS:
              /var/ossec/bin/ossec-control stop

 - La configuraciÃ³n puede ser leÃ-da Ã³ mofificada en /var/ossec/etc/ossec.conf


    Gracias por usar OSSEC HIDS.
    Si tuviera Usted alguna duda, sugerencia Ã³ haya encontrado
    algun desperfecto, contactese con nosotros a contact@ossec.net
    Ã³ usando nuestrs lista pÃºblica de correo en ossec-list@ossec.net

    MÃ¡s informaciÃ³n puede ser encontrada en http://www.ossec.net

            ---  Presione ENTER para finalizar. ---
       (Tal vez encuentre mÃ¡s informaciÃ³n a continuaciÃ³n).
```

Figura 37-2: Resúmen de Instalación del Agente OSSEC
Realizado por: Pazmiño, J; Pazmiño, C. 2018

A continuación, se debe añadir un agente en el correlacionador de eventos y extraer una llave para el mismo, la cual le permitirá cifrar todas las conexiones entre esta comunicación. De tal manera, como se muestra en la figura 38-2.

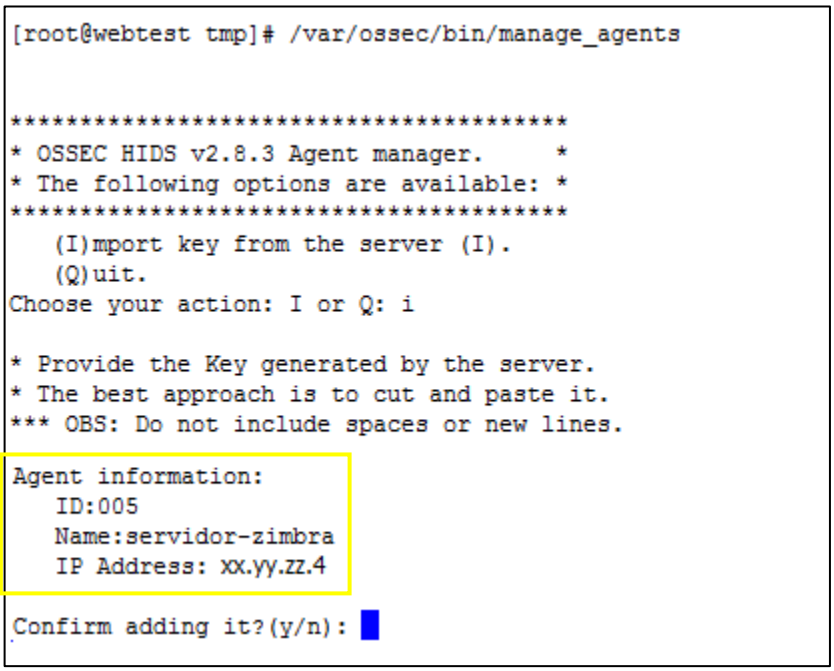


Figura 38-2: Añadimos el Agente en el Servidor OSSEC
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Luego se proporciona un número de identificación por cada agente que deseemos añadir al servidor. Como se muestra en la figura 39-2.

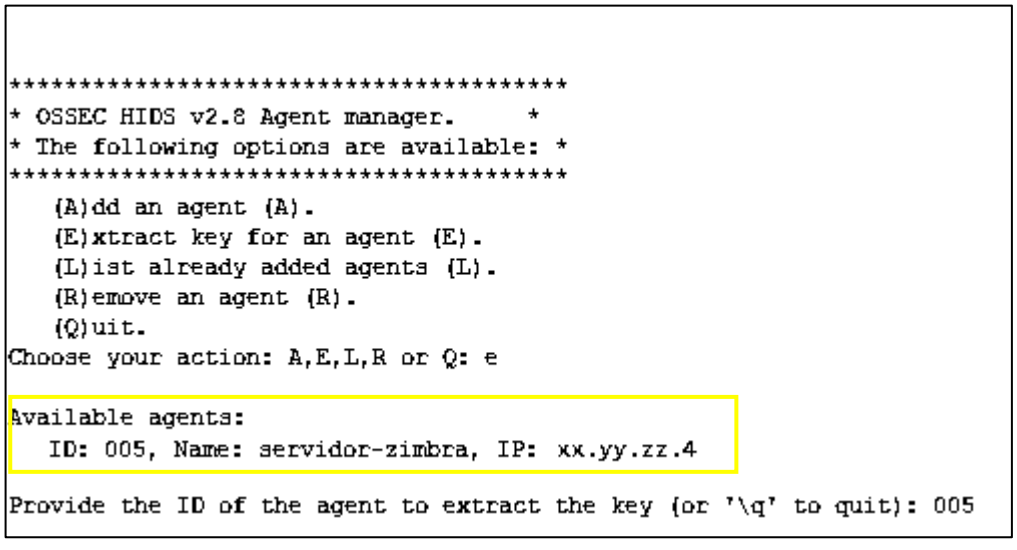


Figura 39-2: Identificación por cada agente
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Posteriormente ingresamos en el servidor la llave generada, como se muestra en la figura 40-2.

Figura 40-2: Generación y copiado de llave
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Añadimos las reglas necesarias en el firewall del correlacionador, para que se establezca la comunicación, como se muestra en la figura 41-2.

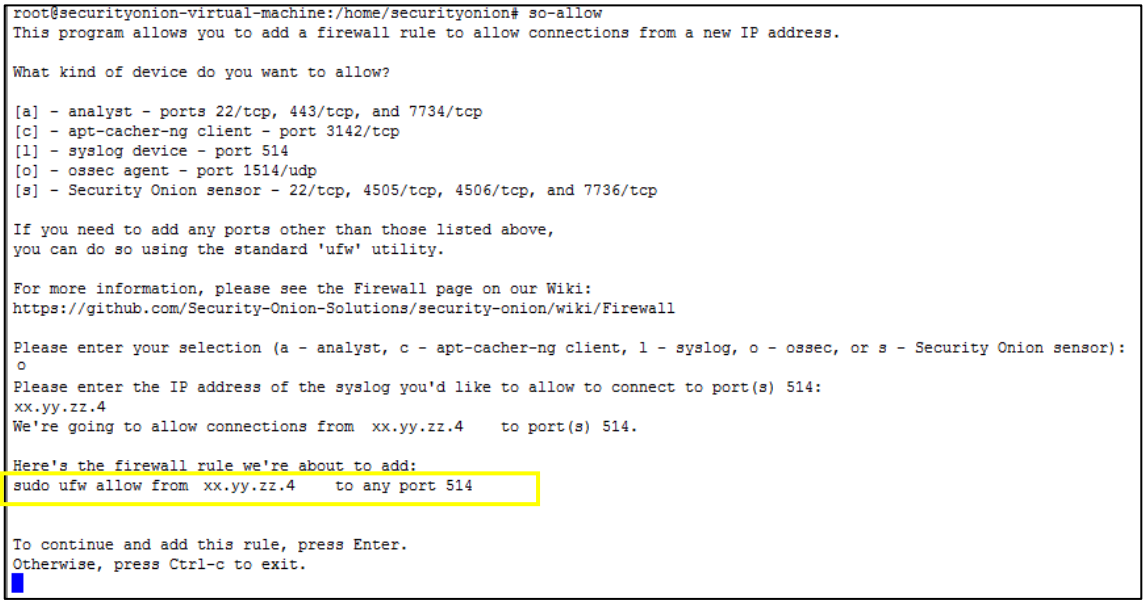


Figura 41-2: Regla para permitir el tráfico
Realizado por: Pazmiño, J; Pazmiño, C. 2018

2.4.5 Configuración de Syslog en los Switch

Para analizar los logs de los switchs en la red, en este caso de la marca CISCO, debemos configurar el estándar de envió de mensajes syslog. De acuerdo con la figura 42-2, se muestra el procedimiento de configuración el mismo que fue replicado en todos los siguientes switchs:

- SW_Gerencia_EERSA
- SW_Contabilidad_2960
- EDF-ANT
- Switch

```
SW_Gerencia_EERSA(config)#
SW_Gerencia_EERSA(config)#logging host xx.yy.zz.50
SW_Gerencia_EERSA(config)#logg
SW_Gerencia_EERSA(config)#logging mon
SW_Gerencia_EERSA(config)#logging monitor
SW_Gerencia_EERSA(config)#
```

Figura 42-2: Configuración Syslog en el Switch de Gerencia
Realizado por: Pazmiño, J; Pazmiño, C. 2018

Luego establecemos el nivel de detalle que deseamos que sea registrada en los logs, siendo el nivel 7 el más alto, como se muestra en la figura 43-2.

```
SW_Gerencia_EERSA(config)#
SW_Gerencia_EERSA(config)#logging trap 7
SW_Gerencia_EERSA(config)#
```

Figura 43-2: Privilegios de Configuración en el Switch de Gerencia
Realizado por: Pazmiño, J; Pazmiño, C. 2018

CAPÍTULO III

3. ANÁLISIS Y RESULTADOS

En el presente capítulo se muestra los datos obtenidos y analizados a través del correlacionador de eventos, en los cuales se puede apreciar el tráfico generado y los ataques informáticos recibidos en la infraestructura de red de la "Empresa Eléctrica Riobamba S.A" durante los meses de enero y febrero de 2018 en las 24 horas del día.

3.1. Recolección de logs

Durante el lapso antes mencionado, se ha recolectado tráfico de red, que corresponde a los siguientes protocolos: SSHD, TELNET, FTP, DNS, HTTP, tal como se detalla en el Gráfico 1-3

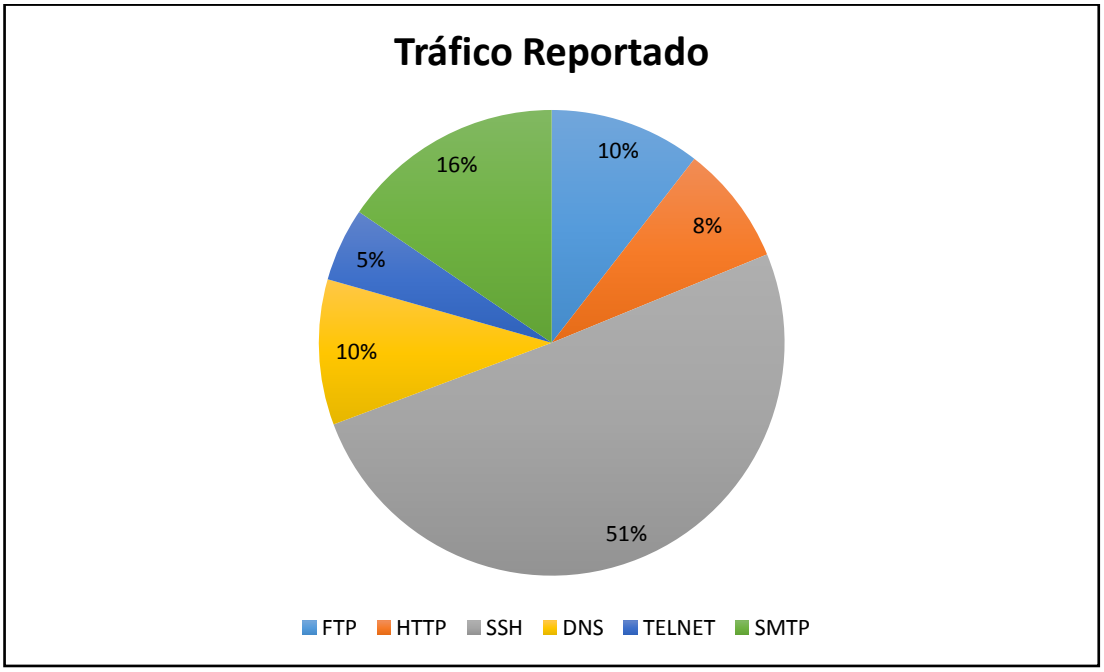


Gráfico 1-3: Tráfico Reportado
Realizado por: Pazmiño, J; Pazmiño, C. 2018

En base al tráfico analizado, en la Tabla 1-3, se detallan los principales ataques informáticos y el número de intentos a la infraestructura de red de la "Empresa Eléctrica Riobamba S.A" en el periodo de tiempo antes mencionado.

Tabla 1-3: Número de Ataques Informáticos Detectados

Ataque informático	Número de intentos	Valor Porcentual
Denegación de servicio	2049	36,59%
Ataques de fuerza bruta	1910	34,11%
Ataques de diccionario	1006	17,96%
Mail Spoofing	345	6,18%
Otros	289	5,16%
TOTAL	**5599**	**100%**

Realizado por: Pazmiño, J; Pazmiño, C. 2018

En el Gráfico 2-3 se muestra el valor porcentual de los ataques informáticos detectados por el correlacionador de eventos.

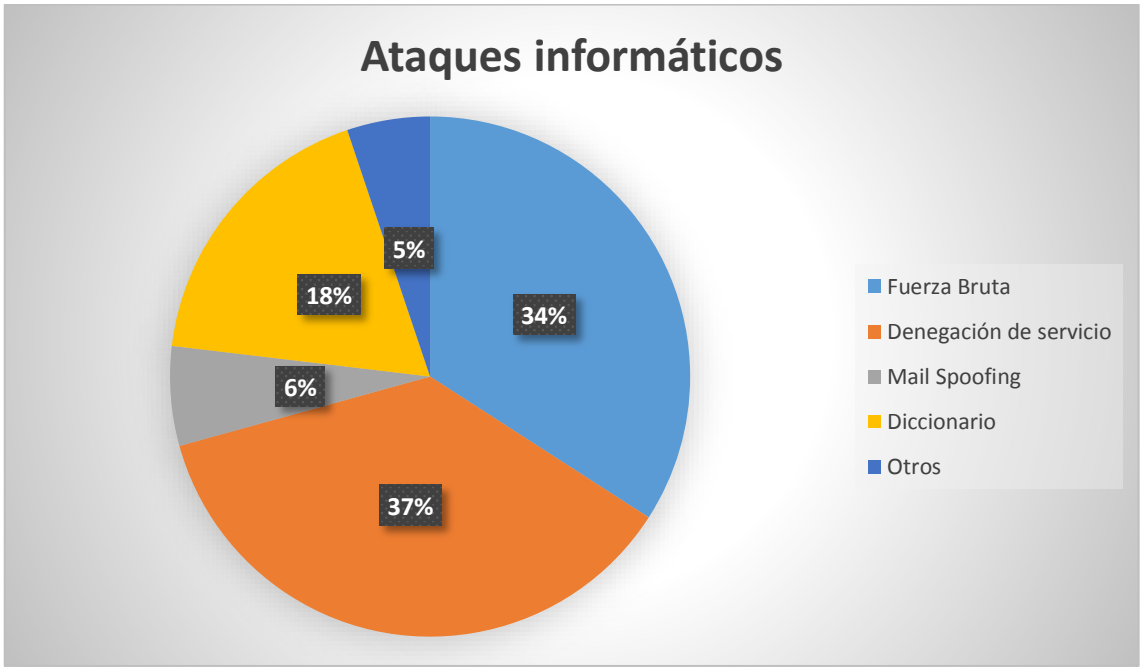
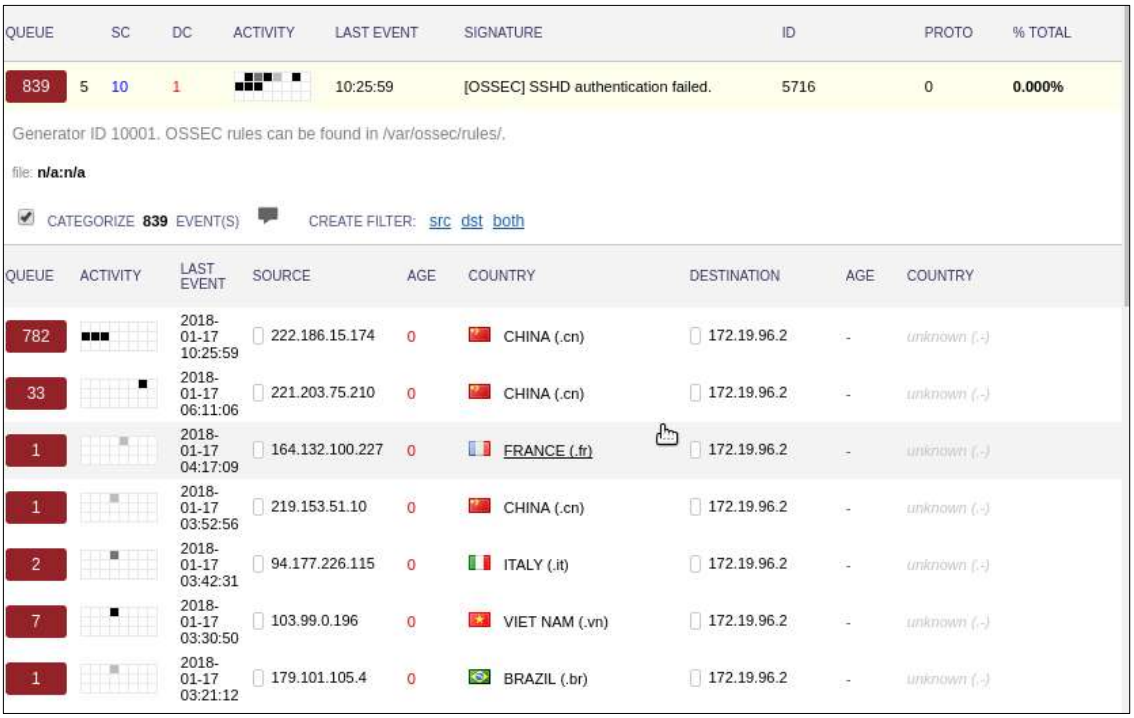


Gráfico 2-3: Tipos de ataques informáticos detectados

Realizado por: Pazmiño, J; Pazmiño, C. 2018

3.2. Ataques informáticos detectados

La Figura 1-3 muestra los intentos de acceso en el módulo de autenticación del servidor de correo electrónico mediante ataques de diccionario, además es posible determinar la dirección IP, geolocalización, número de incidentes, detalle del tráfico generado y hora de cada uno de los incidentes reportados



QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
839	5	10	1	10:25:59	[OSSEC] SSHD authentication failed.	5716	0	0.000%

Generator ID 10001. OSSEC rules can be found in /var/ossec/rules/.

file: **n/a:n/a**

CATEGORIZE **839** EVENT(S) CREATE FILTER: src dst both

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
782		2018-01-17 10:25:59	222.186.15.174	0	CHINA (.cn)	172.19.96.2	-	unknown (-)
33		2018-01-17 06:11:06	221.203.75.210	0	CHINA (.cn)	172.19.96.2	-	unknown (-)
1		2018-01-17 04:17:09	164.132.100.227	0	FRANCE (.fr)	172.19.96.2	-	unknown (-)
1		2018-01-17 03:52:56	219.153.51.10	0	CHINA (.cn)	172.19.96.2	-	unknown (-)
2		2018-01-17 03:42:31	94.177.226.115	0	ITALY (.it)	172.19.96.2	-	unknown (-)
7		2018-01-17 03:30:50	103.99.0.196	0	VIET NAM (.vn)	172.19.96.2	-	unknown (-)
1		2018-01-17 03:21:12	179.101.105.4	0	BRAZIL (.br)	172.19.96.2	-	unknown (-)

Figura 1-3: Ataque de diccionario al servidor de correo
Realizado por: Pazmiño, J; Pazmiño, C. 2018

El 17 de Enero del 2018, se registran incidentes al servidor de correo, con direcciones IP de Holanda. El mismo tráfico que ha sido analizado por el SIEM, de tal manera, como se muestra en la figura 2-3.

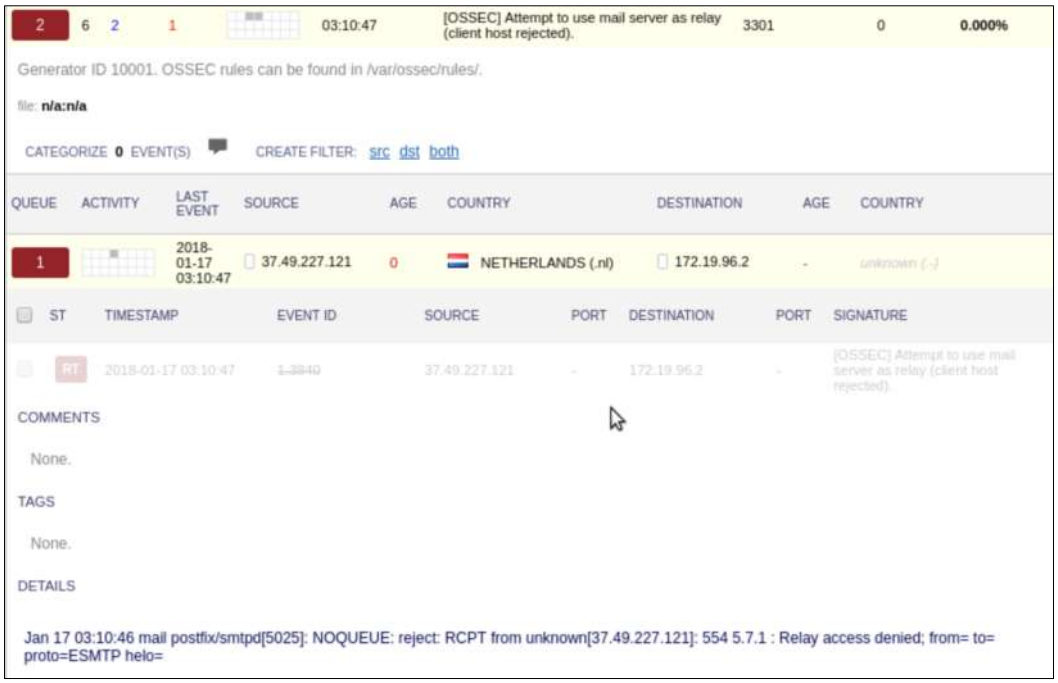


Figura 2-3: Incidencias en el servidor de correo
Realizado por: Pazmiño, J; Pazmiño, C. 2018

En la Figura 3-3 se detalla un ataque de fuerza bruta para vulnerar el servicio de ssh en el servidor de correo electrónico.

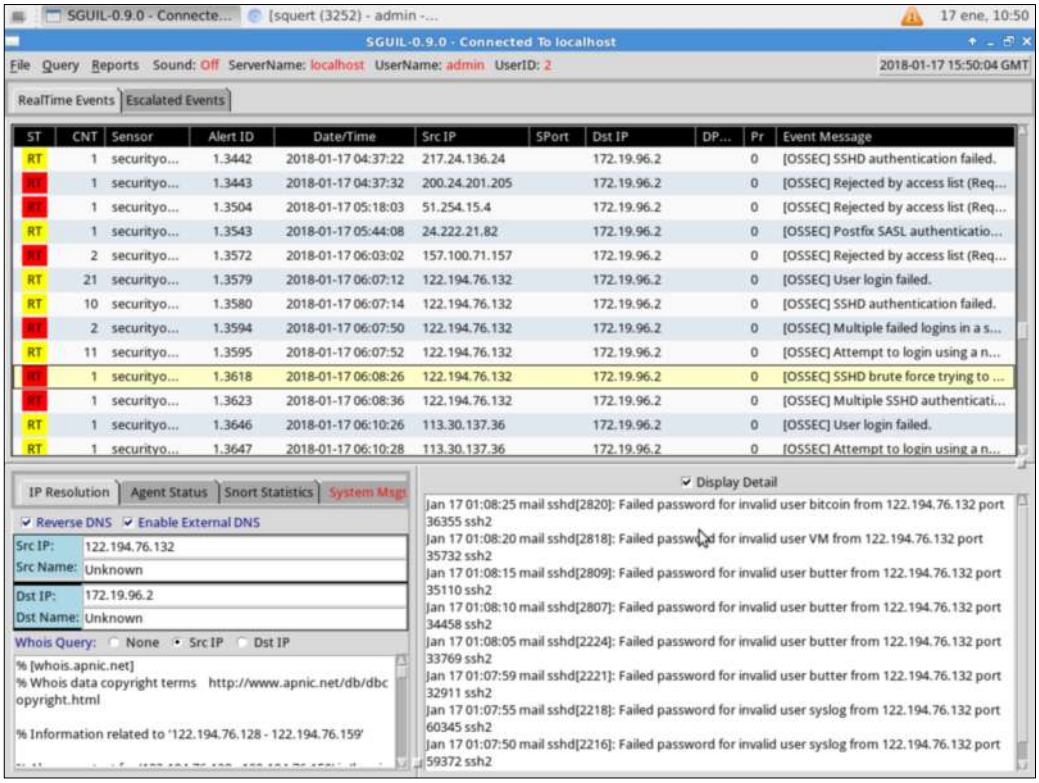


Figura 3-3: Ataque de fuerza bruta al servidor de correo electrónico a través de ssh
Realizado por: Pazmiño, J; Pazmiño, C. 2018

En la Figura 4-3, se detalla un ataque de fuerza bruta al servidor de correo electrónico con el fín de acceder a la cuenta de despacho desde una ip interna.

Figura 4-3: Ataque de fuerza bruta desde una ip interna al servidor de correo electrónico
Realizado por: Pazmiño, J; Pazmiño, C. 2018

En la Figura 5-3, se muestra ataques de diccionario con el fin de obtener acceso al servicio SSH del servidor de cocinas de inducción.

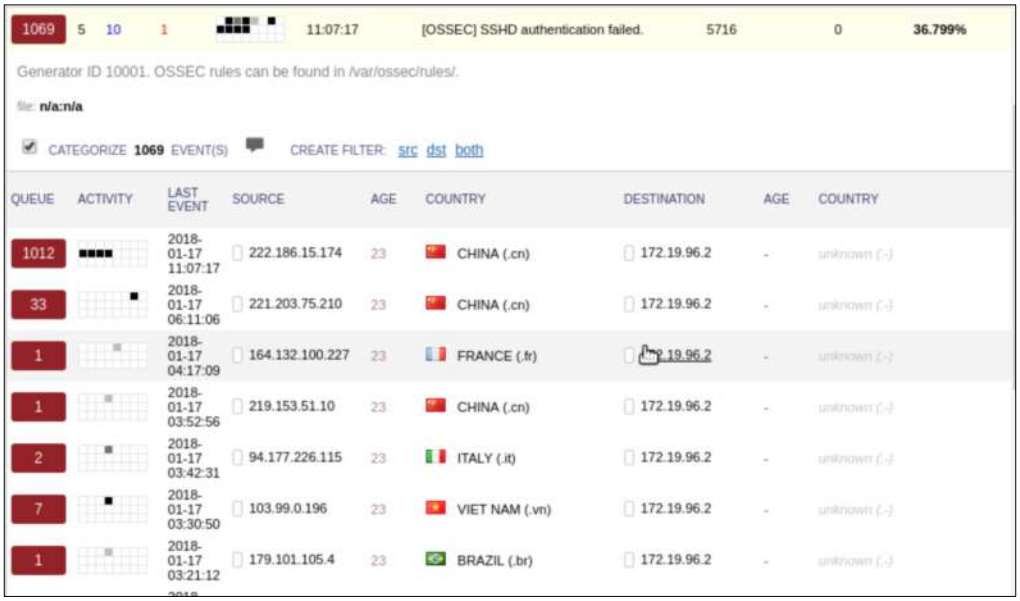
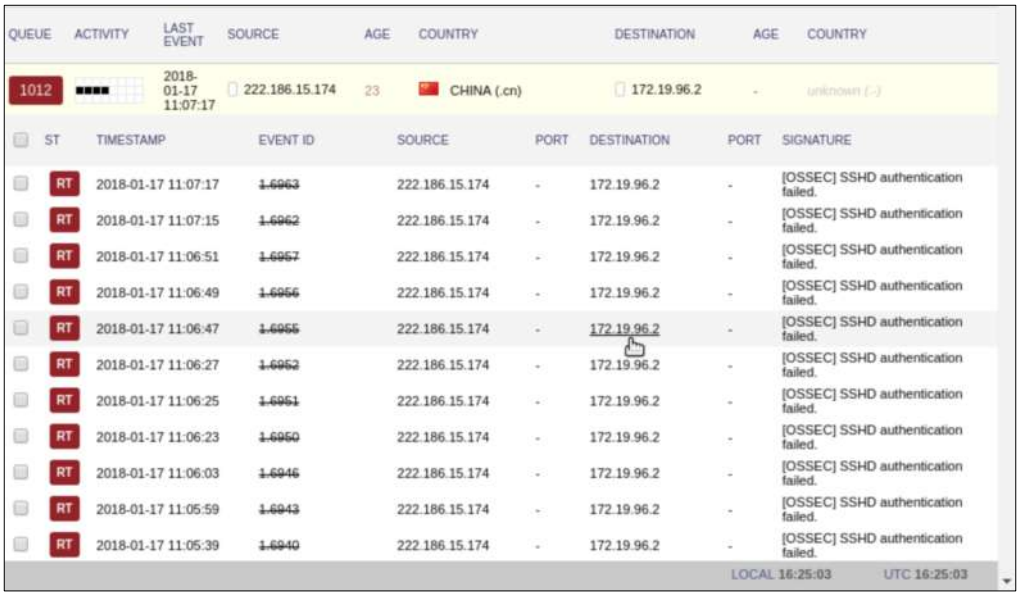


Figura 5-3: Ataque de diccionario al servidor de cocinas de inducción
Realizado por: Pazmiño, J; Pazmiño, C. 2018

La Figura 6-3, detalla los intentos generados desde CHINA por obtener acceso al servidor de correo electrónico el día 17 de enero del 2018.



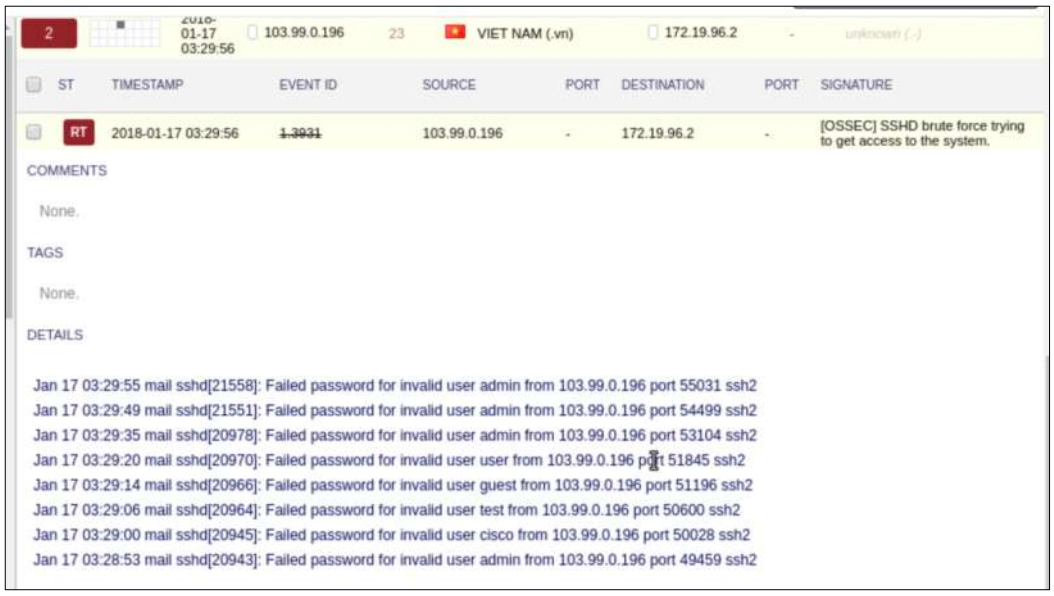
QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
1012	▪▪▪▪	2018-01-17 11:07:17	222.186.15.174	23	CHINA (.cn)	172.19.96.2	-	unknown (..)

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
RT	2018-01-17 11:07:17	1.6963	222.186.15.174	-	172.19.96.2	-	[OSSEC] SSHD authentication failed.
RT	2018-01-17 11:07:15	1.6962	222.186.15.174	-	172.19.96.2	-	[OSSEC] SSHD authentication failed.
RT	2018-01-17 11:06:51	1.6957	222.186.15.174	-	172.19.96.2	-	[OSSEC] SSHD authentication failed.
RT	2018-01-17 11:06:49	1.6956	222.186.15.174	-	172.19.96.2	-	[OSSEC] SSHD authentication failed.
RT	2018-01-17 11:06:47	1.6955	222.186.15.174	-	172.19.96.2	-	[OSSEC] SSHD authentication failed.
RT	2018-01-17 11:06:27	1.6952	222.186.15.174	-	172.19.96.2	-	[OSSEC] SSHD authentication failed.
RT	2018-01-17 11:06:25	1.6951	222.186.15.174	-	172.19.96.2	-	[OSSEC] SSHD authentication failed.
RT	2018-01-17 11:06:23	1.6950	222.186.15.174	-	172.19.96.2	-	[OSSEC] SSHD authentication failed.
RT	2018-01-17 11:06:03	1.6946	222.186.15.174	-	172.19.96.2	-	[OSSEC] SSHD authentication failed.
RT	2018-01-17 11:05:59	1.6943	222.186.15.174	-	172.19.96.2	-	[OSSEC] SSHD authentication failed.
RT	2018-01-17 11:05:39	1.6940	222.186.15.174	-	172.19.96.2	-	[OSSEC] SSHD authentication failed.

LOCAL 16:25:03 UTC 16:25:03

Figura 6-3: Ataques de diccionario generados desde CHINA al servidor de correo
Realizado por: Pazmiño, J; Pazmiño, C. 2018

En la Figura 7-3, se muestra un ataque de fuerza bruta realizado desde VIETNAM con objetivo el servidor de facturación.



2	▪	2018-01-17 03:29:56	103.99.0.196	23	VIET NAM (.vn)	172.19.96.2	-	unknown (..)

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
RT	2018-01-17 03:29:56	1.3931	103.99.0.196	-	172.19.96.2	-	[OSSEC] SSHD brute force trying to get access to the system.

COMMENTS

None.

TAGS

None.

DETAILS

Jan 17 03:29:55 mail sshd[21558]: Failed password for invalid user admin from 103.99.0.196 port 55031 ssh2
Jan 17 03:29:49 mail sshd[21551]: Failed password for invalid user admin from 103.99.0.196 port 54499 ssh2
Jan 17 03:29:35 mail sshd[20978]: Failed password for invalid user admin from 103.99.0.196 port 53104 ssh2
Jan 17 03:29:20 mail sshd[20970]: Failed password for invalid user user from 103.99.0.196 port 51845 ssh2
Jan 17 03:29:14 mail sshd[20966]: Failed password for invalid user guest from 103.99.0.196 port 51196 ssh2
Jan 17 03:29:06 mail sshd[20964]: Failed password for invalid user test from 103.99.0.196 port 50600 ssh2
Jan 17 03:29:00 mail sshd[20945]: Failed password for invalid user cisco from 103.99.0.196 port 50028 ssh2
Jan 17 03:28:53 mail sshd[20943]: Failed password for invalid user admin from 103.99.0.196 port 49459 ssh2

Figura 7-3: Ataque de fuerza bruta al servidor de facturación
Realizado por: Pazmiño, J; Pazmiño, C. 2018

3.3. Incidencias en los activos

En la Tabla 2-3, se detalla el número y tipo de ataques que recibieron los servidores en el tiempo analizado:

Tabla 2-3: Tabla de Incidendias en los Activos

	Facturación	Correo Electrónico	Cocinas de Inducción	DNS	TOTAL
Denegación de servicio	310	1136	470	133	2049
Fuerza Bruta	225	1461	192	32	1910
Mail Spoofing	0	345	0	0	345
Diccionario	96	871	39	0	1006
Otros	0	0	0	289	289
TOTAL	631	3813	701	454	5599

Realizado por: Pazmiño, J; Pazmiño, C. 2018

El valor porcentual de ataques informáticos realizados sobre los activos de la "EERSA" se detalla en el Gráfico 3-3, siendo el servidor de correo electrónico el servidor con mayor número de incidencias.

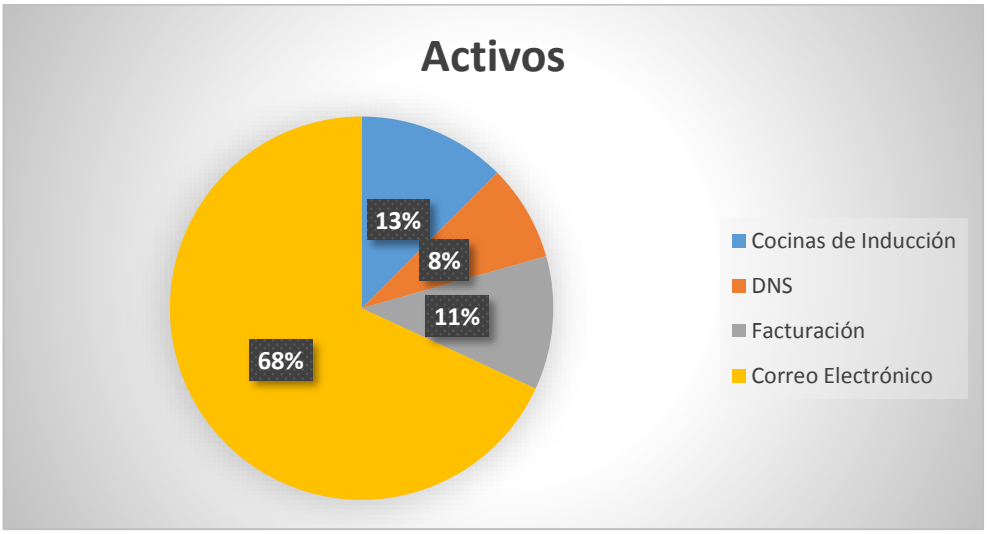


Gráfico 3-3: Ataques informáticos detectados sobre los activos

Realizado por: Pazmiño, J; Pazmiño, C. 2018

3.4. Incidencias por países

Los países que más incidencias generaron en el correlacionador de eventos se muestran en la Tabla 3-3

País	Número de ataques
China	1862
Vietnam	73
Canadá	60
Francia	54
Ecuador	38
Holanda	31

Tabla 3-3: Número de ataques e incidentes por País
Realizado por: Pazmiño, J; Pazmiño, C. 2018

En el Gráfico 4-3, se detalla las principales fuentes de ataques informáticos y su número de intentos.

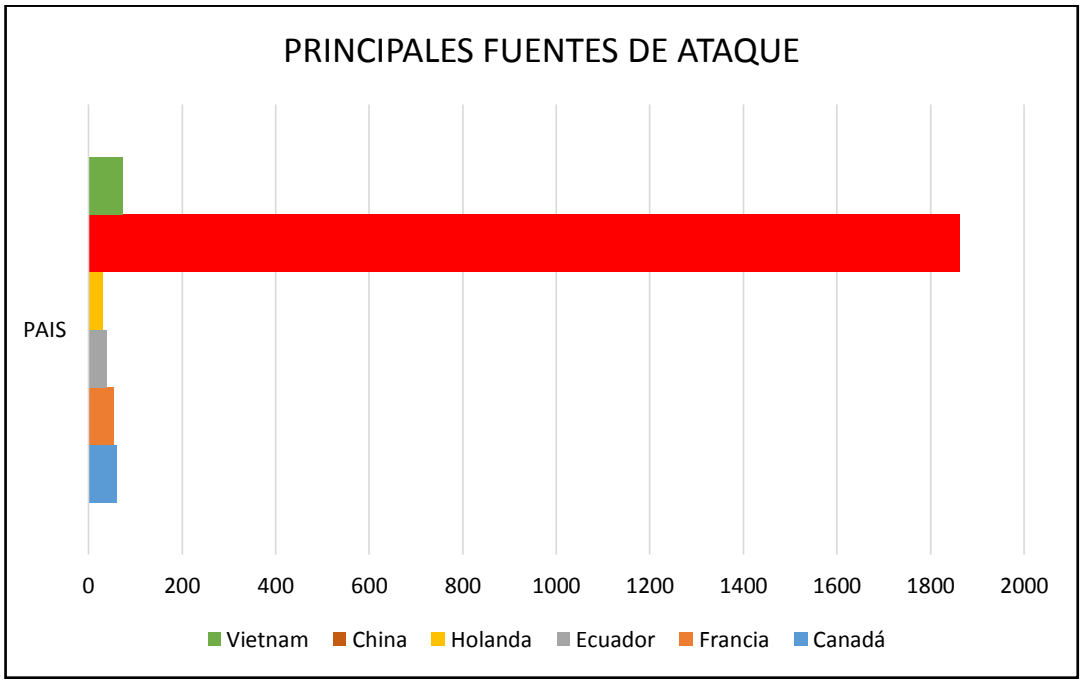


Gráfico 4-3: Fuente de ataques informáticos
Realizado por: Pazmiño, J; Pazmiño, C. 2018

A través del análisis realizado en la recolección de logs de los distintos equipos de red se ha demostrado de esta manera que la implementación del correlacionador de eventos permitirá mejorar la seguridad informática a través de la detección de ataques informáticos en tiempo real.

CONCLUSIONES

- El total de ataques informáticos reportados por el Correlacionador de eventos en el periodo que se tomó de muestra, se pudo determinar que los principales ataques cometidos contra la infraestructura informática de la EERSA son: denegación de servicio y ataques de fuerza bruta con un total de 2049 y 1910 incidencias respectivamente.

- A través de la comparativa realizada se concluye que el sistema operativo "Security Onion" es el que nos presenta mejores herramientas y almacenamiento de registros, los mismos que pueden ser utilizados para un posterior análisis forense.

- Mediante la implementación del Correlacionador de Eventos, se logró determinar que el 51% del tráfico reportado corresponde al protocolo SSH, el cual se debe a la gran cantidad de ataques informáticos en los servidores de la red a través de este servicio en tanto que el activo con el mayor número de incidencias es el servidor de correo electrónico con un número de 3813 que representan el 68% del total de ataques informáticos reportados por el correlacionador de eventos.

- En base a los resultados obtenidos se pudo concluir que el correlacionador de eventos funciona de una manera correcta, detectando ataques en tiempo real y a su vez generando las respectivas alertas; logrando así analizar el tráfico que circula por la red.

RECOMENDACIONES

- Se recomienda verificar la disponibilidad de actualizaciones para el sistema "Security Onion" cada cierto tiempo, ya que al ser un sistema de software libre, se encuentra mejorando constantemente.

- El correlacionador de eventos gestiona, analiza y procesa una gran cantidad de tráfico de la red por lo que, sería recomendable aumentar la memoria RAM del servidor donde se realizó la implementación con el objetivo de que el sistema funcione a su máxima capacidad y no se ralentice.

- En consecuencia, del tráfico que se recoge se recomienda que el tamaño de los discos duros asignados al correlacionador de eventos posean una gran capacidad de almacenamiento y procesamiento.

- Al momento de implementar SPAN se recomienda analizar el porcentaje de procesamiento de los equipos, ya que si excede de un 80% podría ocasionar un mal funcionamiento de la red.

- Con el fin de reducir el número de ataques informáticos de otros países hacia la infraestructura de red de la "EERSA", se recomienda proporcionar los servicios únicamente a nivel de Latinoamérica y bloquear todos los intentos de conexión exteriores, a través de la creación de reglas en el firewall.

- Tener especial cuidado al momento de la generación de las llaves de OSSEC para los agentes, ya que todas las conexiones y envíos de registros serás cifrados a través de esta.

- Se recomienda continuar con la investigación e incluir el procesamiento y estandarización de los logs de los sistemas "SCADA" que se encuentran en la "EERSA", a través del correlacionador de eventos.

BIBLIOGRAFÍA

ALFARO, G. *Prevención de ataques de Cross-Site Scripting en aplicaciones Web*. [En línea]. Barcelona-España 2007. [Consulta: 5 de febrero 2018]. Disponible en: http://www-public.tem-tsp.eu/~garcia_a/web/papers/recsi08-xss.pdf

ALIENVAULT ACADEMY, S. *AlienVault Certified Security Engineer*, 2014, pp.1–134.

BAHIT, E. (2012). *Prevención de ataques por fuerza bruta y Man in the Middle*. [En línea]. 2012. [Consulta: 5 de febrero 2018]. Disponible en: http://46.101.4.154/Art%C3%ADculos%20t%C3%A9cnicos/Seguridad%20Inform%C3%A1tica/Prevenci%C3%B3n%20de%20ataques%20por%20fuerza%20bruta%20y%20Man%20in%20the%20Middle.pdf

BARROS, Rubén & PÉREZ, Pablo. *¿Qué impacto ha tenido el ciberincidente de WannaCry en nuestra economía?* [En línea]. junio 2017. [Consulta: 2 de febrero 2018]. Disponible en: https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/deloitte-analytics/Estudios/Informe-detallado-Ataque%20masivo-Ransomware-WannaCry-finales.pdf

BELISARIO, Aymara. *ANÁLISIS DE MÉTODOS DE ATAQUES DE PHISHING (Trabajo de Titulación)(Especialización en Seguridad Informática)(Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería)*. Buenos Aires: UNIVERSIDAD DE BUENOS AIRES, 2014. pp. 8-10. Disponible en: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0840_BelisarioMendezAN.pdf.

BENCHIMOL, D. *Hacking desde Cero*. [En línea]. 2011 [Consulta: 31 de enero 2018]. Disponible en: http://www.tugurium.com/docs/HakingCero.pdf

BORGHELLO, C. *Cronología de los virus informáticos* [En línea]. 2006 [Consulta: 1 de febrero 2018]. Disponible en: http://marcomp.awardspace.com/descargas/cronologia_virus_inf.pdf

BURKS, D. *Security Onion Wiki.* [En línea]. 2017. [Consulta: 6 de febrero 2018] Disponible en: https://github.com/Security-Onion-Solutions/security-onion/wiki/

CARO, M. *CIBERSEGURIDAD, RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO* [En línea]. 2010 [Consulta: 31 de enero 2018]. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

GÓMEZ, A. *TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS* [En línea]. 2014 [Consulta: 1 de febrero 2018]. Disponible en: http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf.

HEERDEN et al, *AUTOMATED CLASSIFICATION OF COMPUTER NETWORK ATTACKS* [En línea]. 2013 [Consulta: 8 de febrero 2018] Disponible en: https://doi.org/10.1109/ICASTech.2013.6707510

HERNÁNDEZ, C. *Los clanes de la ReD* [En línea]. 2000 [Consulta: 31 de enero 2018]. Disponible en: http://www.tugurium.com/docs/Hackers1_LosClanesDeLaReD2000_ClaudioHernandez.pdf

KANNAN, K. *Top 10 Open Source security tools* [En línea]. 2014 [Consulta: 3 de febrero 2018] Disponible en: http://opensourceforu.com/2014/02/top-10-open-source-security-tools/

LOREDO, Jesús & RAMÍREZ, Aurelio. *DELITOS INFORMÁTICOS: SU CLASIFICACIÓN Y UNA VISIÓN GENERAL DE LAS MEDIDAS DE ACCIÓN PARA COMBATIRLO* [En línea]. 2013 [Consulta: 2 de febrero 2018] Disponible en: http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

MACÍA, Gabriel. *ATAQUES DE DENEGACIÓN DE SERVICIO A BAJA TASA CONTRA SERVIDORES (Trabajo de Titulación)(Departamento de Teoría de la Señal, Telemática y Comunicaciones).* Granada: UNIVERSIDAD DE GRANADA, 2007. pp 35-37. Disponible en: http://digibug.ugr.es/bitstream/10481/1543/1/16714763.pdf

MAMAMI, D. *Fases de un Ataque Hacker* [En línea]. 2013 [Consulta: 5 de febrero 2018] Disponible en: http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a29.pdf.

MIERES, J. *Ataques informáticos* [En línea]. 2009 [Consulta: 1 de febrero 2018]. Disponible en: https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

MUÑOZ et al. *OSSIM OPEN SOURCE SECURITY INFORMATION MANAGEMENT - DESCRIPCIÓN GENERAL DEL SISTEMA* [En línea]. 2003 [Consulta: 6 de febrero 2018] Disponible en: https://www.alienvault.com/docs/OSSIM-desc-es

OSSEC. *OSSEC DOCUMENTATION OFICIAL*. [En línea]. 2017. [Consulta: 4 de febrero 2018]. Disponible en: https://ossec.github.io/docs/manual/

PÁRRIZAS, Ángel. *PROPUESTA DE UNA ARQUITECTURA DE SISTEMAS DE DETECCIÓN DE INTRUSOS CON CORRELACIÓN.(Trabajo de Titulación)(Ingeniería Telemática)(Escuela Técnica Superior de Ingeniería).* Valencia: UNIVERSIDAD DE VALENCIA, 2005. pp.39-40 . Disponible en: http://www.angelalonso.es/doc-

presentaciones/aalonso-PFC.pdf

PAZMIÑO, Luis. *DISEÑO DE UNA METODOLOGÍA PARA LA DETECCIÓN DE ATAQUES A INFRAESTRUCTURAS INFORMÁTICAS BASADA EN LA CORRELACIÓN DE EVENTOS. (Trabajo de maestría) (Instituto de Postgrado y Educación Continua)*. Riobamba: ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO, 2017. pp.41. Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/7817/1/20T00931.pdf

PEDROZA, Juan. *IMPLEMENTACIÓN DE UN GESTOR DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE EVENTOS (SIEM).(Trabajo de Titulación)(Especialización en Seguridad Informática)(Facultad de Ingenierías).* Medellín: UNIVERSIDAD DE SAN BUENA AVENTURA MEDELLÍN, 2016. pp.15. Disponible en: http://bibliotecadigital.usb.edu.co/bitstream/10819/3944/1/Implementacion_Gestor_Seguridad_Pedroza_2016.pdf

TELEFÓNICA. *Qué es el Email Spoofing y cómo evitarlo con el registro SPF*. [En línea]. 2017. [Consulta: 5 de febrero 2018] Disponible en: https://www.acens.com/wp-content/images/2017/12/spoofing-wp-acens.pdf

ANEXOS

ANEXO A

ARCHIVO DE CONFIGURACIÓN DE INTERFACES

/etc/networking

```
# This configuration was created by the Security Onion setup script.
#
# The original network interface configuration file was backed up to:
# /etc/network/interfaces.bak.
#
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# loopback network interface
auto lo
iface lo inet loopback

# Management network interface
auto eth0
iface eth0 inet static
  address xx.yy.zz.50
  gateway xx.yy.zz.1
  netmask 255.255.255.0
  dns-nameservers xx.yy.zz.7
  dns-domain eersa.com.ec

auto eth1
iface eth1 inet manual
  up ip link set $IFACE promisc on arp off up
  down ip link set $IFACE promisc off down
  post-up ethtool -G $IFACE rx 4096; for i in rx tx sg tso ufo gso gro lro; do ethtool -K $IFACE
$i off; done
  post-up echo 1 > /proc/sys/net/ipv6/conf/$IFACE/disable_ipv6
```

ANEXO B

ARCHIVO DE CONFIGURACIÓN EN EL SERVIDOR DE OSSEC

/var/ossec/etc/ossec.conf

root@securityonion-ProLiant-DL380-G5:/home/securityonion# cat /var/ossec/etc/ossec.conf

```
<!-- OSSEC example config -->

<ossec_config>
  <global>
    <email_notification>no</email_notification>
    <logall>yes</logall>
  </global>

  <syslog_output>
      <server>127.0.0.1</server>
  </syslog_output>

  <rules>
    <include>rules_config.xml</include>
    <include>pam_rules.xml</include>
    <include>sshd_rules.xml</include>
    <include>telnetd_rules.xml</include>
    <include>syslog_rules.xml</include>
    <include>arpwatch_rules.xml</include>
    <include>symantec-av_rules.xml</include>
    <include>symantec-ws_rules.xml</include>
    <include>pix_rules.xml</include>
    <include>named_rules.xml</include>
    <include>smbd_rules.xml</include>
    <include>vsftpd_rules.xml</include>
    <include>pure-ftpd_rules.xml</include>
    <include>proftpd_rules.xml</include>
    <include>ms_ftpd_rules.xml</include>
    <include>ftpd_rules.xml</include>
    <include>hordeimp_rules.xml</include>
    <include>roundcube_rules.xml</include>
    <include>wordpress_rules.xml</include>
    <include>cimserver_rules.xml</include>
    <include>vpopmail_rules.xml</include>
    <include>vmpop3d_rules.xml</include>
    <include>courier_rules.xml</include>
    <include>web_rules.xml</include>
    <include>web_appsec_rules.xml</include>
    <include>apache_rules.xml</include>
    <include>nginx_rules.xml</include>
    <include>php_rules.xml</include>
    <include>mysql_rules.xml</include>
    <include>postgresql_rules.xml</include>
    <include>ids_rules.xml</include>
```

```
  <include>squid_rules.xml</include>
  <include>firewall_rules.xml</include>
  <include>cisco-ios_rules.xml</include>
  <include>netscreenfw_rules.xml</include>
  <include>sonicwall_rules.xml</include>
  <include>postfix_rules.xml</include>
  <include>sendmail_rules.xml</include>
  <include>imapd_rules.xml</include>
  <include>mailscanner_rules.xml</include>
  <include>dovecot_rules.xml</include>
  <include>ms-exchange_rules.xml</include>
  <include>racoon_rules.xml</include>
  <include>vpn_concentrator_rules.xml</include>
  <include>spamd_rules.xml</include>
  <include>msauth_rules.xml</include>
  <include>mcafee_av_rules.xml</include>
  <include>trend-osce_rules.xml</include>
  <include>ms-se_rules.xml</include>
  <!-- <include>policy_rules.xml</include> -->
  <include>zeus_rules.xml</include>
  <include>solaris_bsm_rules.xml</include>
  <include>vmware_rules.xml</include>
  <include>ms_dhcp_rules.xml</include>
  <include>asterisk_rules.xml</include>
  <include>ossec_rules.xml</include>
  <include>attack_rules.xml</include>
  <include>local_rules.xml</include>
  <include>securityonion_rules.xml</include>
</rules>

<syscheck>
  <!-- Frequency that syscheck is executed -->
  <frequency>25200</frequency>

  <!-- Directories to check  (perform all possible verifications) -->
  <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
  <directories check_all="yes">/bin,/sbin</directories>
  <directories check_all="yes">/var/ossec/etc</directories>

  <!-- Files/directories to ignore -->
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>
  <ignore>/etc/mail/statistics</ignore>
  <ignore>/etc/random-seed</ignore>
  <ignore>/etc/adjtime</ignore>
  <ignore>/etc/httpd/logs</ignore>
</syscheck>

<rootcheck>
  <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
</rootcheck>

<global>
```

```
  <white_list>127.0.0.1</white_list>
</global>

<remote>
  <connection>secure</connection>
</remote>

<alerts>
  <log_alert_level>1</log_alert_level>
  <email_alert_level>7</email_alert_level>
</alerts>

<command>
  <name>host-deny</name>
  <executable>host-deny.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>firewall-drop</name>
  <executable>firewall-drop.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>disable-account</name>
  <executable>disable-account.sh</executable>
  <expect>user</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

<!-- Active Response Config -->
<active-response>
  <!-- This response is going to execute the host-deny
     - command for every event that fires a rule with
     - level (severity) >= 6.
     - The IP is going to be blocked for  600 seconds.
    -->
  <command>host-deny</command>
  <location>local</location>
  <level>6</level>
  <timeout>600</timeout>
</active-response>

<active-response>
  <!-- Firewall Drop response. Block the IP for
     - 600 seconds on the firewall (iptables,
     - ipfilter, etc).
    -->
  <command>firewall-drop</command>
  <location>local</location>
  <level>6</level>
```

```
  <timeout>600</timeout>
</active-response>

<!-- Files to monitor (localfiles) -->

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/messages</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/secure</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/xferlog</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/mail.err</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/mail.log</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/syslog</location>
</localfile>

<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/error.log</location>
</localfile>

<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/other_vhosts_access.log</location>
</localfile>

<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/snorby_access.log</location>
</localfile>
```

```
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/snorby_error.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/ssl_access.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/xplico_access.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/xplico_error.log</location>
  </localfile>

  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>

  <localfile>
    <log_format>command</log_format>
    <command>/usr/sbin/sostat-interface</command>
    <alias>packets_received</alias>
    <frequency>600</frequency>
  </localfile>

<!--Address xx.yy.zz.14 added by /usr/sbin/so-allow on vie ene 19 18:05:33 UTC 2018-->
  <global>
    <white_list> xx.yy.zz.14</white_list>
  </global>

<!--Address xx.yy.zz.40 added by /usr/sbin/so-allow on vie ene 19 18:39:38 UTC 2018-->
  <global>
    <white_list> xx.yy.zz.40</white_list>
  </global>
</ossec_config>
```