ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

DIRECCIÓN DE POSGRADO Y FORMACIÓN CONTINUA

INFORME DE INVESTIGACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN TECNOLOGÍA DE LA INFORMACIÓN MENCIÓN REDES Y SISTEMAS DISTRIBUIDOS

MODALIDAD:

PROYECTO DE INVESTIGACIÓN Y DESARROLLO

TEMA:

PLAN DE FORTALECIMIENTO ANTE ATAQUES INFORMÁTICOS DEL HOSPITAL DE ESPECIALIDADES PORTOVIEJO BASADOS EN SISTEMAS DE CORRELACIÓN DE LOG

AUTORES:

ING. ANDY ALCIDES MORA CRUZATTY

ING. JOSÉ DAVID VILLACRESES CHANCAY

TUTOR:

CESAR MOREIRA ZAMBRANO. Mgtr.

CALCETA, MAYO 2022

DERECHOS DE AUTORÍA

ANDY ALCIDES MORA CRUZATTY y **JOSÉ DAVID VILLACRESES CHANCAY**, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, que se han respetado los derechos de autor de terceros, por lo que asumimos la responsabilidad sobre el contenido del mismo, así como ante la reclamación de terceros, conforme a los artículos 4, 5 y 6 de la Ley de Propiedad Intelectual.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido en el artículo 46 de la Ley de Propiedad Intelectual y su Reglamento.

Firmado electrónicamente por:
ANDY ALCIDES MORA CRUZATTY

Andy Alcides Mora Cruzatty

JOSE DAVID VILLACRESES CHANCAY

Firmado digitalmente por JOSE DAVID VILLACRESES CHANCAY
Fecha: 2022.05.25 09:06:40 -05'00'

José David Villacreses Chancay

CERTIFICACIÓN DE TUTOR

Mgtr. CESAR MOREIRA ZAMBRANO, certifica haber tutelado el Trabajo de Titulación **PLAN DE FORTALECIMIENTO ANTE ATAQUES INFORMÁTICOS DEL HOSPITAL DE ESPECIALIDADES PORTOVIEJO BASADOS EN SISTEMAS DE CORRELACIÓN DE LOG**, que ha sido desarrollado por **ANDY ALCIDES MORA CRUZATTY Y JOSÉ DAVID VILLACRESES CHANCAY**, previa la obtención del título de Magister en Tecnologías de la Información, mención Redes y Sistemas Distribuidos de acuerdo con el REGLAMENTO DE LA UNIDAD DE TITULACIÓN DE LOS PROGRAMAS DE POSGRADO de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

CESAR ARMANDO MOREIRA ZAMBRANO

Firmado digitalmente por CESAR ARMANDO MOREIRA ZAMBRANO
Fecha: 2022.05.24 19:28:05 -05'00'

Mgtr. CESAR MOREIRA ZAMBRANO

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaramos que hemos **APROBADO** el trabajo de titulación **PLAN DE FORTALECIMIENTO ANTE ATAQUES INFORMÁTICOS DEL HOSPITAL DE ESPECIALIDADES PORTOVIEJO BASADO EN SISTEMAS DE CORRELACIÓN DE LOG**, que ha sido propuesto, desarrollado y sustentado por **ANDY ALCIDES MORA CRUZATTY** Y **JOSÉ DAVID VILLACRESES CHANCAY**, previa la obtención del título de Magister en Tecnología de la Información mención Redes y Sistemas Distribuidos, de acuerdo al Reglamento de la unidad de titulación de los programas de Posgrado de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

RAMON AGUSTIN VARELA MUNOZ
Firmado digitalmente por RAMON AGUSTIN VARELA MUNOZ

MGTR. RAMÓN VARELA MUÑOZ
MIEMBRO

GUSTAVO GABRIEL MOLINA GARZON
Firmado digitalmente por GUSTAVO GABRIEL MOLINA GARZON
DN: C=EC, SN=MOLINA GARZON, G=GUSTAVO GABRIEL, SERIALNUMBER=IDCEC-1307723286, CN=GUSTAVO GABRIEL MOLINA GARZON, OID.2.5.4.97=TINEC-1307723286001
Razón: Estoy aprobando este documento
Ubicación: la ubicación de su firma aquí
Foxit PDF Reader Versión: 11.2.1

MGTR. GABRIEL GUSTAVO MOLINA GARZÓN
MIEMBRO

Firmado electrónicamente por:
RAMON JOFFRE MOREIRA PICO

MGTR. RAMÓN JOFFRE MOREIRA PICO
PRESIDENTE

AGRADECIMIENTO

Mi agradecimiento, va dirigido a Dios, por ser la principal guía y así poder finalizar esta importante etapa de mi vida académica.

A mi mamá que ha sido mi fortaleza con apoyo incondicional juntos a mis hermanos y demás familiares que siempre estuvieron presentes día a día.

A esta prestigiosa universidad ESPAM MFL, que me acogió y me permitió ser parte de ella para forjar un futuro dentro de sus instalaciones.

A mi tutor el Ing. Cesar Moreira, quien con sus conocimientos y orientaciones me ayudó en el desarrollo del proyecto de titulación y culminarlo satisfactoriamente.

A mis amigos y compañeros quienes me acompañaron en esta gran etapa y que de una u otra forma me brindaron su apoyo.

José David Villacreses Chancay

AGRADECIMIENTO

Mis agradecimientos, van dirigidos en primer lugar, a Dios, por ser el principal guía y así poder finalizar esta importante etapa de nuestras vidas.

A mis padres, esposa, hija, hermana y demás miembros de mi familia, siendo ellos el motor que hace desear superarme y crecer profesional y personalmente día a día.

A esta prestigiosa Universidad ESPAM MFL, que me acogió y permitió ser parte de ella para afianzar y adquirir nuevos conocimientos dentro de sus instalaciones.

A mi tutor y maestro Ing. César Moreira, quien con sus conocimientos y orientaciones me ayudó en el desarrollo del proyecto de titulación y culminarlo satisfactoriamente.

De manera muy especial agradezco al Hospital de Especialidades Portoviejo quienes brindaron las facilidades para la ejecución del proyecto y así poder culminarlo.

Andy Alcides Mora Cruzatty

DEDICATORIA

Quiero dedicar de manera muy especial este trabajo principalmente a Dios, quien deposito en mí la fuerza de voluntad para culminar un importante logro.

A mi papa que esta junto a Dios y mi mamá quienes siempre estuvieron a mi lado brindándome su apoyo incondicional, por su dedicación y ejemplo de vida.

A mis hermanos, sobrinos y amigos que de una u otra manera siempre estuvieron presentes y apoyándome desinteresadamente.

José David Villacreses Chancay

DEDICATORIA

Quiero dedicar de manera muy especial este trabajo principalmente a Dios, quien deposito en mí la fuerza de voluntad para culminar un objetivo más.

A mis padres y esposa quienes siempre estuvieron a mi lado brindándome su apoyo incondicional, siendo mi principal fuente motivacional para mi superación.

A mi hija Daniela como muestra de superación y voluntad para seguir adelante, preparándose es la manera de superar los obstáculos que se presenten en la vida, así como la satisfacción de superación personal y profesional.

A mis amigos y compañeros que de una u otra manera siempre estuvieron presentes y apoyándome en la etapa de preparación.

Andy Alcides Mora Cruzatty

CONTENIDO GENERAL

CONTENIDO DE TABLAS, FIGURAS Y ANEXOS

RESUMEN

Las redes tecnológicas simbolizan para las instituciones un activo importante para operar y gestionar los datos y servicios por ellos brindados, en este sentido el Hospital de Especialidades Portoviejo, posee varios dispositivos computacionales en los que sustenta sus actividades, así mismo la institución no cuenta con un instrumento centralizado de monitoreo y prevención ante ataques informáticos. El objetivo de este proyecto fue la preparación de un plan de mejoras ante ataques informáticos del Hospital de Especialidades Portoviejo basado en sistemas de correlación de logs. La metodología que se utilizó fue PPDIOO la misma que contempla las fases de: Preparación, Planificación, Diseño, Implementación, Operación y Optimización, aplicado a los sistemas de correlación de eventos Security Information and Event Management (SIEM) utilizando el sistema AlienVault OSSIM, el cual permite comparar, integrar y visualizar incidentes de seguridad en tiempo real, permitiendo implementar estrategias de defensa en profundidad. Como resultado de la investigación se estableció un plan de mejoras para fortalecer la infraestructura de red actual del Hospital de Especialidades Portoviejo ante ataques informáticos y como conclusiones, se puede señalar que la utilización de la herramienta AlienVault OSSIM hizo posible mejorar los mecanismos de ciberseguridad garantizando la integridad, seguridad, y disponibilidad de la información, evitando así anomalías en la red y fallos en sus servicios, dichos mecanismos combinados con diferentes herramientas de monitoreo y detección integradas permiten tener una gestión centralizada de la seguridad dentro de la Institución.

PALABRAS CLAVE

Redes, Monitoreo, SIEM, Kernel, OSSIM, Logs, Ataques Informáticos, Buffer, Denegación de Servicio, Overflow, Fuerza bruta, Defensa en Profundidad, Correlación de Eventos.

ABSTRACT

The technological infrastructures represent for the current institutions an asset of extreme importance in order to manipulate and manage the information, in this sense El Hospital de Especialidades Portoviejo, has a significant quantity and variety of technological instruments for the support of its daily activities, likewise this institution does not have a centralized tool for monitoring and preventing computer attacks. The objective of this research was the elaboration of an improvement plan to prevent and repeal computer attacks of the Hospital de Especialidades Portoviejo based on log correlation systems. The methodology used in the research was PPDIOO which includes the phases of: Preparation, Planning, Design, Implementation, Operation and Optimization, applied to the Security Information and Event Management (SIEM) event correlation systems using the AlienVault OSSIM system, which allows comparing, integrating and visualizing security incidents in real time, allowing the implementation of a depth strategy for defense. As a result of the investigation, an improvement plan was established to strengthen the current infrastructure of the Hospital de Especialidades Portoviejo against computer attacks, the conclusion of the research noticed that: the use of the OSSIM tool made it possible to improve cybersecurity mechanisms guaranteeing security, integrity and availability, thus avoiding anomalies in the network and failures in its services, combined with different integrated monitoring and detection tools, allowing for centralized security management within the Institution.

KEY WORDS

Networks, Monitoring, SIEM, Kernel, OSSIM, Logs, Computer Attacks, Buffer, Denial of Service, Overflow, Brute Force, Defense in Depth, Correlation of Events.

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

Actualmente dependemos cada vez más y en mayor medida de la tecnología, los ataques informáticos son complejos y difíciles de ser detectados. La información es considerada un activo crítico de la organización el cual juega un papel estratégico para todas las instituciones, se debe garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información almacenada en ellas.

Davyt (2017), manifiesta que cada vez es evidente que los mecanismos de seguridad se han incrementado de una manera considerable en los servicios de red desde servidores y otros dispositivos, por lo cual es necesario aplicar estrategias de seguridad como herramientas para la detección de virus y acceso a la información.

Según Goldman & Feldman (2021), define que “la funcionalidad del entorno, los sistemas de atención, la comunicación entre los proveedores y muchos otros factores pueden, en última instancia, afectar a la seguridad del paciente”, esto quiere decir que es indudable que cada vez aparecen nuevos peligros en la privacidad de la informática como un nuevo espacio en los riesgos que inciden en la seguridad.

Godoy (2020), manifiesta que los centros de salud con ayuda de otras instituciones, se han puesto en alerta sobre un posible ataque cibernético en contra de instituciones de salud y empresas proveedoras de servicios médicos; el ataque denomidado ransomware es según Godoy (2020) “un virus informático que bloquea las computadoras y los datos de un sistema hasta que se paga un rescate” es decir se considera como un peligro amenazador y puede causar amenazas en la atención médica y financieros.

Según estudios realizados en América Latina por la compañía de seguridad rusa Karspesky en el año 2019, señala que, el sector salud fue uno de los más atacados

por los hackers en 2019, los costos de un ciberataque al sector son elevados, debemos señalar que los datos manejados en dicho ámbito deben ser de estricta confidencialidad y muy perceptivos (Hernandez , 2019). La amenaza puede presentarse en países subdesarrollados y de gran desarrollo como América Latina y el Caribe, esto se debe a la falta de estrategias oportunas antes estos peligros que afectan la información (Raudales, 2017) .

Ecuador no está fuera de su alcance cuando se trata de ciberataques. En 2015, un ciberataque contra el Banco del Austro (BDA) le costó al banco 12 millones de dólares (Insurance Journal, 2016). El ataque tuvo como objetivo los servidores de BDA y ordenó a Wells Fargo que realizara transferencias de dinero a una cuenta bancaria en Hong Kong (Tom Bergin & Nathan Layne, 2016), en julio del 2021 la Corporación Nacional de Telecomunicaciones (CNT) fue víctima de un ciberataque (Ransomware) provocando fallas en sus sistemas vulnerando diversas instancias como el sitio web, la red, base de datos y sistemas informáticos.

Actualmente, los sistemas del Hospital de Especialidades Portoviejo (HEP) mantienen ambientes tecnológicos diferentes tanto de producción, pruebas y desarrollo, con sus respectivas bases de datos. Así mismo las bases de datos del hospital por el hecho de contener información confidencial de los pacientes no son compartidas con otras instituciones, salvo los reportes necesarios y solicitados por parte de entidades de carácter superior como Ministerio de Salud Pública (MSP).

La infraestructura tecnológica actual con la que cuenta el HEP es considerada estándar, es decir, cuenta con dispositivos de seguridad perimetral y configuraciones de seguridad informática independientes entre cada una de ellas, estos dispositivos generan gran cantidad de logs los mismos que no son analizados para una correcta administración de los eventos ocurridos en la red.

Con los precedentes enunciados se presenta la siguiente interrogante:

¿De qué manera contribuir a la seguridad perimetral ante ataques informáticos en el data center del Hospital de Especialidades Portoviejo?

1.2. JUSTIFICACIÓN

La presente investigación determina que la seguridad informática es el proceso de proteger la información de toda organización para mantener la seguridad, prestigio, procesamiento y evitar el manejo de los datos, es por esto que la importancia de la Ciberseguridad radica en las consecuencias desastrosas en todas las áreas que puede tener en cualquier organización, provocando problemas financieros como productivos, por ende debe estar dirigida a prevenir amenazas y los posibles riesgos a los sistemas de información organizacionales, no existe actualmente un procedimiento, pero si podemos reducir al máximo la ocurrencia de dichos incidentes (Morales, Toapanta, & Toasa, 2019).

Tomando como base el COIP (Código Orgáncio Integral Penal, 2014), podemos citar varios artículos: **La Interceptación ilegal de datos, Artículo 230** señala “Será sancionada…La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático”. **La Transferencia electrónica de activo patrimonial, Artículo 231** señala que “La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos…” **El Ataque a integridad de sistemas informáticos, Artículo 232** indica que “La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos…será sancionada con pena privativa de libertad de tres a cinco años”. **Acceso no consentido a sistemas informáticos**, **Artículo 234** puntualiza “La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho…será sancionada con la pena privativa de la libertad de tres a cinco años”.

En el aspecto ambiental la consecuencia de la ejecución de un plan de fortalecimiento ante ataques informáticos basados en la correlación de logs a aplicarse en el data center del Hospital de Especialidades Portoviejo, permitirá un consumo de energía eficiente pues no será necesario la compra de equipos especializados que consuman grandes cantidades de energía, de la misma forma el prever los posibles ataques informáticos permitirá el uso y desempeño normal de los equipos informáticos y de networking de la institución.

A nivel social, la disertación y análisis de los sistemas de correlación sirve como aporte al fortalecimiento de la seguridad perimetral y la prevención de accesos anómalos hacia la infraestructura tecnológica, beneficiando al centro de datos del Hospital de Especialidad Portoviejo y a su vez a los usuarios y pacientes de esta casa de salud, adicional aquello se establecerán políticas de acceso y de denegación basados en eventos de logs generados por los servidores. Una solución de seguridad centralizada permite minimizar los riesgos de vulnerabilidad y penetración hacia los servidores y dispositivos activos que forman parte de la infraestructura de red basado en herramientas de correlación de logs.

En consecuencia el impacto económico del proyecto se verá reflejado en minimizar los costos generados en el caso de un incidente de ciberseguridad como son recuperación ante desastres, compra de software especializado, compra de equipos especializados, entre otros. Además, se denota el acompañamiento y asesoramiento del Tutor para la elaboración de la investigación.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Diseñar un plan de fortalecimiento ante ataques informáticos basado en correlación de logs para contribuir con el afianzamiento de la seguridad perimetral en el Data Center del Hospital de Especialidades Portoviejo.

1.3.1. OBJETIVOS ESPECÍFICOS

- Realizar un análisis de la seguridad cibernética e infraestructura tecnológica del data center del Hospital de Especialidades Portoviejo.
- Establecer elementos de un sistema de seguridad centralizado y correlación de eventos de logs.
- Implementar un sistema de seguridad centralizado y correlación de logs
- Generar ataques cibernéticos en un ambiente controlado y ambiente de producción para verificar fortaleza del sistema de seguridad centralizada y correlación de logs.
- Elaborar un plan de fortalecimiento ante ataques informáticos basado en correlación de logs.

1.4. IDEA A DEFENDER

La implementación de un sistema de seguridad centralizada y correlación de logs permitirá mejorar la seguridad dentro del Centro de Datos del Hospital de Especialidades Portoviejo

CAPITULO II. REVISIÓN BIBLIOGRÁFICA

2.1. ATAQUES INFORMÁTICOS

La realidad actual es la interconexión y dependencia de la tecnología, por lo cual las intromisiones informáticas se vuelven más complicadas y difíciles de detectar, las diversas formas de negociar, están asociadas a diferentes tipos de datos que se generan en cada acción o transacción suscita un alto grado de atención para obtener el mejor método de protección para dicha información o activo el cual tiene un gran valor cada vez mayor.

Leiva (2015), manifiesta que el ámbito de la tecnología de información es un proceso que permite el manejo de los datos y la comunicación, sin embargo, esto puede causar problemas y conflictos que incidan en la privacidad de los datos de una organización, existen diferentes elementos que favorecen a la propagación de procesos ilícitos en el ciberespacio, en razones financieras, políticas, y procesos de bajo costo que son utilizados para eliminar las amenazas.

Las empresas que han sufrido incidentes de seguridad durante los últimos años tardan mucho tiempo, incluso meses en ser detectados, es claro que la estrategia clásica de defensa mediante el agregado de capas de seguridad no es suficiente, típicamente las organizaciones responden a esta nueva realidad agregando más y más capas de seguridad.

Se estima que más de 940.000 individuos le fueron sustraídos algún tipo de dato o contraseña en el año 2020, los mecanismos usados por delincuentes informáticos es hacer uso de un sin número de combinaciones entre símbolos, letras y números para poder obtener la contraseña adecuada, así mismo estos ciberdelincuentes tienen software especializados para cometer dichos delitos. Otro mecanismo es el denominado *“pishing”*, en que los hackers fingen pertenecer a alguna institución, por lo general bancos. México y Brasil lideran el desarrollo de mecanismos de Ciberseguridad en América Latina (La Republica, 2021).

Partiendo de la premisa en que los sistemas informáticos no son 100% seguros y que el uso de la tecnología en el medio privado o público, puede ser de cierta manera riesgosa, ya que si no se adquieren los equipos y tecnologías necesarias para hacer frente a las amenazas se puede tener un riesgo de seguridad latente que exponga información sensible de la organización o institución; se hace necesario entonces poder contar con la ayuda de un sistema que permita monitorear, comprender y analizar el comportamiento de las redes corporativas y ayude a determinar anomalías en la red, gestionando y controlando ambientes de TI los cuales poseen un gran número de equipos de networking.

2.2. TIPOS DE ATAQUES INFORMÁTICOS

En la actualidad el nivel de complejidad de las Tecnologías de la Información y Comunicación (TICs) ha aumentado, agregando un mayor riesgo para los sistemas informáticos, teniendo como consecuencia el aumento en el número de ataques aprovechando las vulnerabilidades o fallos de seguridad(A. Hernández & Mejía, 2015).

La forma de contrarrestar un ataque informático y prevenirlo es usando técnicas y mecanismos que nos permitan revelar vulnerabilidades a tiempo. Hay varios tipos de ataques por el cual un atacante puede valerse de ellos y podemos nombrar los siguientes:

- A nivel de S.O. (Sistemas Operativos)
- A nivel de capa de aplicación
- A nivel de configuraciones erróneas

2.2.1. A NIVEL DE SISTEMAS OPERATIVOS

En el área de informática, existen riesgos a evaluar en los cuales los sistemas operativos están muy inmersos ya que traen pre-configurados ciertas características que ayudan a incrementar su funcionalidad, cosa que conllevaría a ser propenso a poseer ciertas vulnerabilidades que podrían ser explotadas por presuntos delincuentes

que están en constante búsqueda de estas vulneraciones que están desatendidas por el personal informático o usuario final(CEH, 2020).

Instalaciones y configuraciones por defecto de los sistemas operativos tienen varios puertos y servicios abiertos, estableciendo riesgos de seguridad. La mayoría de parches trata de solventar vulnerabilidades a nivel de sistema operativo, sin embargo, no puede considerarse la aplicación de un parche como una solución de seguridad definitiva(CEH, 2020).

Dentro de las vulneraciones a nivel de sistema operativo tenemos:

- S.O. sin actualizaciones
- S.O. sin parches de seguridad
- Bugs en el S.O.
- Desbordamiento de buffer

2.2.2. A NIVEL DE CAPA DE APLICACIÓN

Este tipo de ataques van dirigidos contra la capa de aplicación, y su objetivo es provocar que el servicio deje de estar operativo, aprovechando para ello deficiencias de diseño en los protocolos de comunicaciones de esta capa o los fallos de diseño o implementación de las propias aplicaciones.(INCIBE, 2015)

Figura 1 Mapa con los ataques DDoS diarios

Fuente: digitalattackmap.com, 2021

Al desarrollar estas prácticas es frecuente complementar con técnicas de especulación. DDoS frente a la capa de aplicación, cuyo objetivo es utilizar la totalidad de la RAM y tiempos de procesamiento necesarios para las actividades normales, minimizando recursos utilizados por el atacante respecto a debilidades de la aplicación, podemos citar las siguientes características:

- Menor consumo de internet, respecto a otros métodos de agresiones SYN Flood.
- Mayor problema al determinar tráfico maligno del legítimo, los mecanismos se centran en capas de red o transporte, poco fiables al ser atacados en la capa de aplicación. Incluso para sistemas de defensa que supervisan esta capa es complicado discernir entre el tráfico malicioso y el legítimo.(INCIBE, 2015)

Entre otros ataques a nivel de capa de aplicación podemos nombrar los siguientes:

- SQL Injection
- Denegación de Servicios DDOS
- Ataques TCP SYN

- Cross Site Scripting
- Ataques Buffer Overflow

La **inyección de SQL** (SQL Injection) ciberataque de tipo encubierto por el que un hacker inyecta su propio código en un sitio web con la finalidad de vulnerar la seguridad y tener acceso a la información protegida, al tener éxito la intromisión puede acceder a la base de datos y secuestrar los datos del usuario(Avast, 2021).

Figura 2. Forma de un ataque SQL Injection

Fuente: Avast.com

El ataque **Cross Site scripting**, más conocido como ataque XSS, es un tipo de vulnerabilidad de las páginas web el cual permite a los atacantes enviar secuencias de códigos maliciosos en los sitios web y aplicaciones que el usuario utiliza, instalando malware en los navegadores y obteniendo acceso a la máquina del usuario(Avast, 2021).

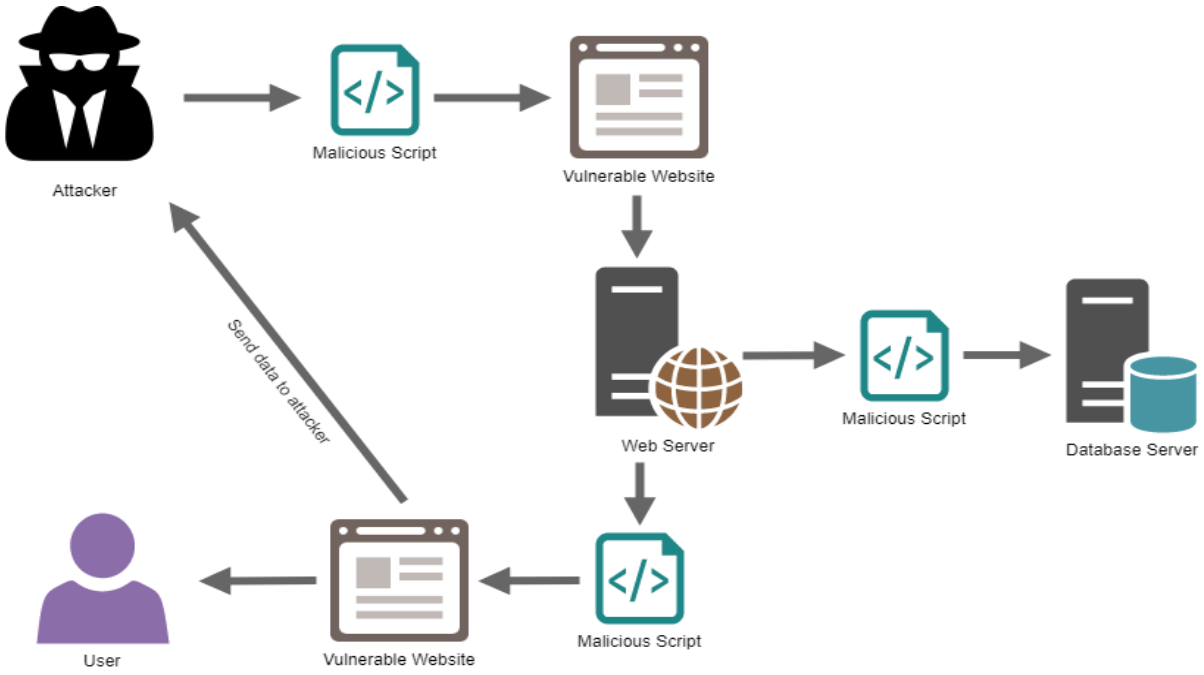


Figura 3. Esquema de una ataque XSS

Fuente: pc-solucion.com, 2020

Un ataque de denegación de servicios DoS, intromisión o ataque que tiene como objetivo final obstruir a un usuario el uso del sistema o recurso para el cual está destinado a ser usado. Las técnicas para estos ataques son: denegación de servicio DoS y denegación de servicio distribuido DDoS. La diferencia entre ambos es el número de ordenadores o IP´s que realizan el ataque(OSI, 2018).

En los ataques DoS se generan una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones, esto es cuando se materializa la denegación del servicio(OSI, 2018).

Entre los ataques DoS mas comunes tenemos los siguientes:

- ✓ Ping de la muerte
- ✓ Slowloris
- ✓ Inundación Syn

- ✓ Inundación de puertos sin servicio
- ✓ Inundación por fragmentos
- ✓ Inundaciones mediante paquetes anómalos
- ✓ Inundación de puertos de servicio
- ✓ Inundación ICMP
- ✓ Inundación Zombie

- **Mecanismo del ataque de inundación SYN**

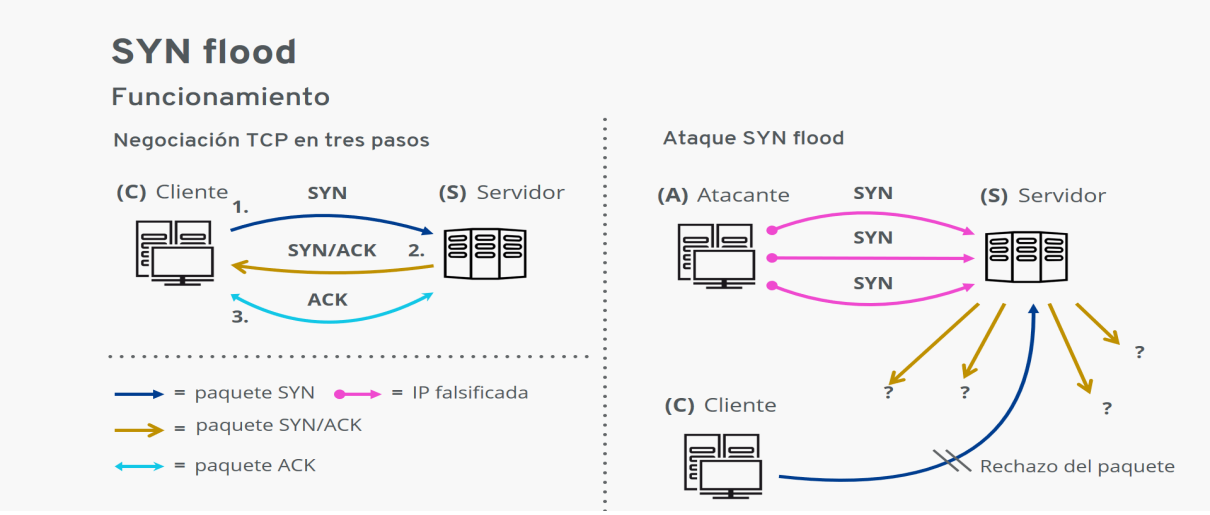


Figura 4. Esquema de ataque SYN
Fuente: (IONOS, 2020)

En la figura 4 se observa el mecanismo de un ataque syn flood, el cual produce la interrupción general de la conexión tcp.

2.2.3. A NIVEL DE CONFIGURACIONES ERRONEAS

Las ineficientes o malas configuraciones en los que se ven afectados los servidores tanto web, aplicación, bases de datos o framework, lo cual podría ocasionar un sinnúmero de accesos ilegales y robo de la información de la empresa sea esta pública o privada, incluso el apoderamiento de todo el complejo de servidores. Si los sistemas están mal configurados lo que llevaría a dar permisos no permitidos a un archivo o aplicación que no debe verse desde internet, no se puede considerar seguro el servidor con la anomalía (Ambit, 2019).

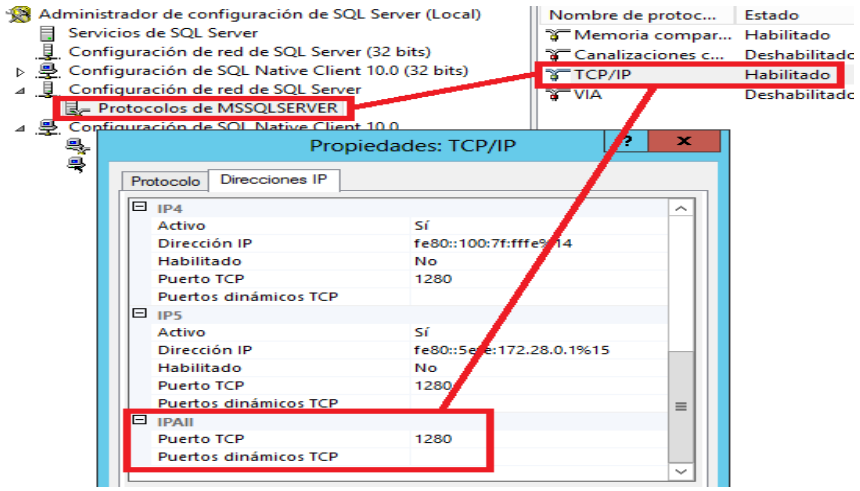


Figura 5. Puerto SQL TCP
Fuente: https://www.sysadmit.com/

2.3. ACTIVIDADES DE LOS ATACANTES INFORMÁTICOS

- **Desfiguramiento de páginas web**: Es muy común, la página principal se cambia o altera, se aprovechan las vulnerabilidades de las aplicaciones (Jhony & Alvarado, 2015).

- **Robo de datos en medios electrónicos**: Los datos pueden ser robados por herramientas de ataques desplegadas en los desfiguramientos de sitios web. Cuando el atacante logra acceso a la red puede tener acceso a información valiosa (Jhony & Alvarado, 2015).

- **Ataques a esquemas instructores del servidor**: Son aquellos que admiten comunicaciones bidireccionales entre servidores - usuarios web, el objetivo es ejecutar comandos, leer o modificar archivos del sistema (Jhony & Alvarado, 2015).

- **Ataques DoS**: el objetivo es impedir la realización de tareas u operaciones, generalmente se logra saturando la red, consumiendo recursos del sistema, errores de programación (Jhony & Alvarado, 2015).

2.3.1. FASES EN UN ATAQUE INFORMÁTICO.

Existen diversas etapas en un ataque informático antes que el atacante emprenda la intrusión:

- **Reconocimiento y gestación**: Inicia identificando y seleccionando el objetivo, recolecta datos para transgredir la seguridad, por lo general la técnica más utilizada es la ingeniería social (Ariu, Frumento, & Fumera, 2017)

- **Distribución y acceso**: El ciberdelincuente utiliza varias herramientas a su disposición, escaneo de puertos, explora debilidades e infecta a su víctima, logrado su objetivo el equipo contaminado aguarda instrucciones de su atacante.

- **Actuación o explotación**: El atacante comienza escaneando y conquistando paquetes, recopilando información, denegando servicios, en si las diferentes acciones que un atacante pueda ocasionar, sustraer credenciales, capturas de pantallas, documentación confidencial, instalar programas, etc.

- **Cubriendo huellas**: El atacante elimina huellas de su intrusión, rastros de operaciones realizadas, mantiene accesos a los sistemas y dispositivos comprometidos, al borrar su rastro el ciberdelincuente pasa desapercibido y el personal de seguridad no contara con certezas o huellas del suceso.

2.4. VULNERABILIDAD TECNOLÓGICA EN LATINOAMÉRICA Y ECUADOR

Con relación a países de Latinoamérica se debe considerar el nuevo espacio geopolítico tecnológico, ha arrancado el consenso de una cultura de seguridad la cual se espera concienciar el acatamiento de normas que promuevan la seguridad de la información, podemos mencionar que los países de Colombia y Brasil son grandes potencias en el área de Ciberseguridad.

Con respecto a la problemática antes mencionada la UNASUR (Unión de Naciones Suramericanas), en su tópico de planes de acción del 2012 al 2014 incluyo esta temática. De tal manera, se definieron mecanismos políticos y capacidades regionales, con raíz de disminuir o detener los intentos de ataques cibernéticos en la región. En el plan del 2015 la temático incluyo el Plan de Acción, para continuar con el trabajo de la defensa contra ataques cibernéticos, la cual fue tomada o adoptada también por la Organización de Estados Americanos (OEA), como estrategia Interamericana Integral de Seguridad Cibernética(Cornaglia & Vercelli, 2017).

Según la estadística de la situación digital de Ecuador en el 2020-2021 se tenía un total de 10.17 millones de usuarios conectados al internet, siendo el 57% de la población quienes tienen acceso a este medio, a enero del 2020 y enero 2021 se tuvo un incremento del 1.5% de usuarios lo que equivale a 147 mil usuarios añadidos (Alvino, 2021).

Ante lo mencionado, se observa que las instituciones financieras y comerciales como: industrias, bancos, casas comerciales, entre otros; han aumentado los servicios en líneas para poder efectuar sus transacciones. Por otra parte, las entidades públicas han implementado nuevos sistemas como el servicio en línea que resulta más ágil para las personas, incrementando la oferta y demanda de sus productos a través del internet.

2.5. METODOLOGÍA DE SIMULACIÓN DE AGRESIONES INFORMÁTICAS

Para simular agresiones informáticas un pentester pretenderá obtener acceso exclusivo a las aplicaciones o sistemas, se lo realiza mediante las siguientes etapas, reconocimiento, escaneo, enumeración, análisis de vulnerabilidad, explotación, reportes, con el objetivo de descubrir falencias en la seguridad y analizar el grado de riesgo y presentar alternativas de solución acorde a la metodología establecida.

2.5.1. METODOLOGÍA OSSTMM (OPEN SOURSE SECURITY TESTING METHODOLOGY MANUAL)

La metodología OSSTMM provee directrices que permiten realizar pruebas y análisis de seguridad publicado bajo “Licencia Creative Commons 3.0”, lo que permite su libre uso y distribución (Herzog, 2010). Se fundamenta para su análisis el cumplimiento de las siguientes directrices:

- ✓ Que se pueda contar
- ✓ Sólido y repetible
- ✓ Mantenible en el tiempo
- ✓ Fundamentado en conocimientos de Pentester
- ✓ Profundo
- ✓ Acorde a leyes y derechos humanos

2.5.2. ESQUEMA DE SEGURIDAD METODOLOGÍA OSSTMM

Se compone por 6 apartados semejantes superpuestos entre sí, conteniendo síntesis de todos los otros apartados; la figura 6 señala el esquema de seguridad con las diversas opciones de observación de la metodología.

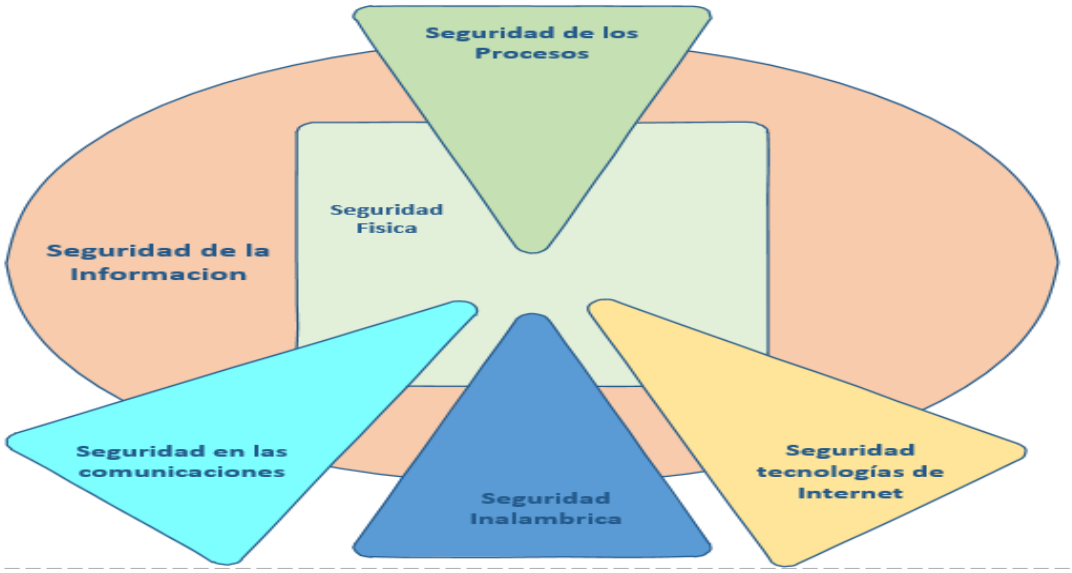


Figura 6. Metodología de Seguridad OSSTMM
Fuente: ISECOM 2010

Las técnicas definidas en el presente esquema componen los aspectos de seguridad que deben ser perfeccionados en el análisis según amerite, tenemos las siguientes:

1. Seguridad de la Información
2. Seguridad de los Procesos
3. Seguridad en las tecnologías de Internet
4. Seguridad en las Comunicaciones
5. Seguridad Inalámbrica
6. Seguridad Física

En la figura 7 se muestran lineamientos y métodos para determinar pruebas en los módulos OSSTMM.

Figura 7. Lineamientos de realización de pruebas
Fuente: ISECOM 2010

Cada módulo de la metodología tiene una entrada y una salida como se muestra en la figura 8, la entrada son datos utilizados en cada proceso y la salida el resultado de labores concluidas.

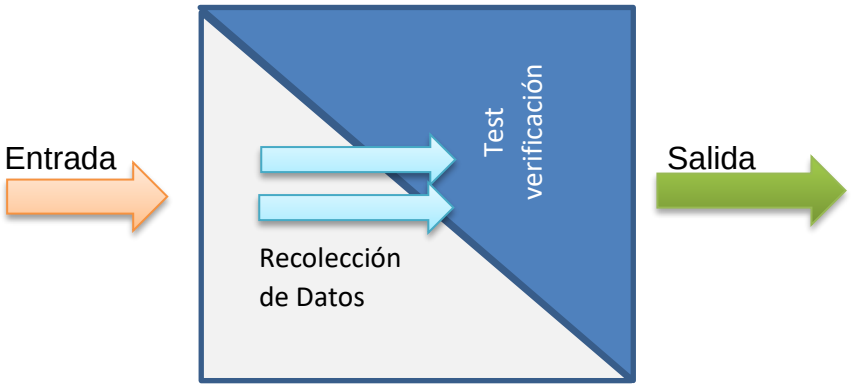


Figura 8 Metodología OSSTMM
Fuente: ISECOM 2010

La salida puede o no ser datos analizados que sirven como entrada para otro módulo o incluso puede ocurrir que la misma salida sirva como entrada para más de un módulo o sección; y las tareas son las pruebas de seguridad a ejecutarse dependiendo de la entrada del módulo, los resultados de las tareas son considerados la salida del módulo y pueden ser analizados inmediatamente para actuar como un resultado procesado o se pueden dejar sin analizar. (Acosta Naranjo, 2013).

2.6. SISTEMAS DE PREVENCIÓN DE ATAQUES SIEM

Los sistemas SIEM son usados para realizar análisis de eventos de seguridad informática aplicado en tiempo real, recolectar y almacenar trazas, permitiendo analizar con técnicas forenses incidentes y permitir el cumplimiento en las regulaciones existentes. Estos sistemas poseen dos funciones principales (Miller, Harris, Harper, Vandyke, & Black, 2010).

Definición de SEM - SIM

- SEM Gestión de Eventos de Seguridad: realiza la monitorización en tiempo real de eventos y la gestión de incidentes, esta función procesa las trazas recogidas de los dispositivos en la red, aplicaciones, sistemas operativos y herramientas de seguridad en tiempo real, para el monitoreo y así garantizar una buena monitorización y dar respuesta a los incidentes previstos

- SIM Gestión de Información de Seguridad: está relacionada al reporte de regulaciones y gestión de las trazas, en la cual se garantizan la recolección, análisis y reportes de los datos de seguridad, las fuentes en las que se obtienen son todo aquello unido a la red y su entorno tanto hardware como software.

Los sistemas SIEM actúan como un repositorio central para las trazas generadas por las diferentes herramientas y permiten seleccionar, a través de reglas lógicas, los eventos de seguridad informática que interesan (Agrawal & Makwana, 2013).

De acuerdo a un estudio de la consultora Gartner (Kavanagh & Rochford, 2015), el mercado de los sistemas SIEM se considera maduro y muy competitivo, encontrándose en una fase de adopción amplia donde múltiples desarrolladores de SIEM ofrecen las funciones básicas de gestión de trazas, monitorización de eventos y cumplimiento de regulaciones.

2.6.1. CORRELACIÓN DE EVENTOS

Generalmente nos proporciona información obtenida de los eventos al identificar situaciones anómalas basadas en incidencias, de esta manera podemos efectuar predicciones y expresar tendencias sobre el futuro en una infraestructura tecnológica. Existen diversos enfoques en la correlación de eventos, como análisis de datos de mercado, detección de fraude (por ejemplo, detectar los patrones de uso infrecuente de una tarjeta de crédito), análisis de logs del sistema (por ejemplo, agrupar mensajes similares y aumento de acontecimientos importantes) o análisis de gestión y fallas de red (por ejemplo, detectar la causa de un problema de red)(Müller, 2009).

2.6.2. ARQUITECTURA GENERAL DE CORRELADORES DE EVENTOS

La arquitectura general que podemos encontrar en los correladores de eventos es la siguiente:

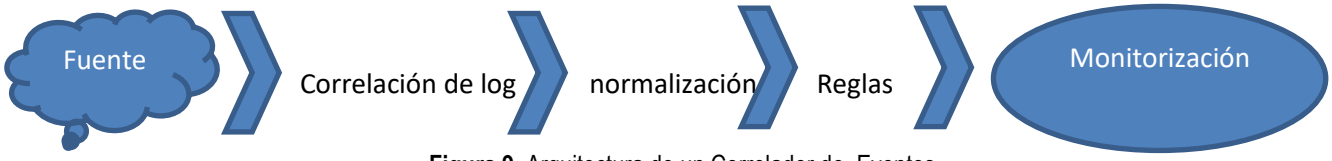


Figura 9. Arquitectura de un Correlador de Eventos
Fuente: Autores

Algunos detalles de este esquema:

- Una fuente o host, que puede ser un ordenador, router, envía su información o eventos al servidor Syslog o a un fichero de texto.
- Se realiza una recolección en un formato determinado (XML, ficheros de texto…).
- Se normalizan para la plataforma o sistema de correlación.
- Se analizan los eventos recibidos y se toma una serie de decisiones:
  - ✓ **Mensaje anulado**. Solo informativos, se descartan y no se almacenan los datos.
  - ✓ **Mensaje almacenado**. Los mensajes que se consideran importantes se almacenan en la base de datos de eventos.
  - ✓ **Alarma**. Al existir un evento generando una alarma esta se almacena, pudiendo generar tareas extras, por ejemplo enviar correos, publicar mensajes en consola, entre otros.
- Y son gestionados por un usuario o sistema final.

A continuación se describen las soluciones SIEM, identificando cada una de ellas si cumplen los criterios de software libre propuesto para el desarrollo de esta investigación.

Tabla 1 Comparativa herramientas Siem.

Herramienta	Fuente	Observaciones	Aplica/No aplica
IBM QRADAR	https://www.ibm.com/es-es/products/qradar-siem	Herramienta de software propietario	No

HP ArcSight	https://www.microfocus.com/es-es/products/siem-security-information-event-management/overview	Herramienta de software propietario	No
Splunk	https://www.splunk.com/en_us/software.html	Herramienta con licencia GNU	Si
SolarWinds	https://www.solarwinds.com/security-event-manager	Herramienta de software propietario	No
AlienVault	https://cybersecurity.att.com/products/ossim	Herramienta que cuenta con la solución OSSIM (open source) con licencia GNU	Si
Mozdef	https://mozdef.readthedocs.io/en/latest/overview.html	Herramienta con licencia GNU	Si
EventTracker	https://www.netsurion.com/managed-threat-protection	Herramienta de software propietario	No

Fuente: Autores.

En la siguiente tabla se realiza una comparativa de las herramientas que aplican Open Source, identificando sus características significativas.

Tabla 2 Comparativas de productos Open Source Siem

Herramienta ***Descripción***	**Splunk**	**AlienVault OSSIM**	**Mozdef**
Basado en GNU	✓	✓	✓
Capacidad de almacenamiento y procesamiento de logs.	Limitada	Limitada	**X**

Transferencia segura de datos	✓	✓	✓
Visualizaciones de estados continuo	✓	✓	✓
Normalizador de Eventos	✓	✓	✓
Balanceo de carga/clúster	✓	✓	✓
Interfaz personalizables	✓	✓	✓
Años de experiencia	15 años	12 años	10 años
Sito web	✓	✓	✓

Fuente: Autores

De acuerdo con análisis y comparativas realizadas tanto de las herramientas Open Source como las de software propietario, se toma en consideración la utilización para esta investigación la solución AlienVault OSSIM, la cual incluye varios componentes usables para el correcto funcionamiento del proyecto y por destacarse en su calificación de prestaciones.

2.7. OSSIM ALIEN VAULT

AlienVault OSSIM (Open Source Security Information Manager) una solución Siem, fue desarrolla en el año 2000, la cual incluye las técnicas de prevención y detección de intrusos en la seguridad general de una red, también funciona a raíz de un conjunto de herramientas de monitoreo y seguridad con licencia GNU (Open Source), tales como Nagios, Snort, Openvas, Ntop, entre otras. Por lo tanto ofrece una gran capacidad y rendimiento en sus análisis, gestión, organización de los eventos que se producen entorno a la red en función, dado que la mayorías de sistemas Siem no dan estas prestaciones, siendo una herramienta factible para su uso por muchos factores ya mencionados (Bowling, 2010).

Algunas de las características principales de OSSIM son:

- Análisis de conducta de red.
- Monitoreo de eventos forenses.
- Observación de peligros de seguridad.
- Genera reportes competentes.
- Tiene un diseño de alto rendimiento.
- Notificaciones automáticas.
- Plugin free.
- Detección de intrusos.
- Es gratuito.

2.7.1. COMPONENTES Y CARACTERÍSTICAS

Dentro de los componentes que conforman la herramienta OSSIM podemos citar:

- **Snort**: Sistema de detección de intrusos con licencia GNU, brinda capacidad de almacenamiento de bitácoras en registros y en bases de datos abiertas (Snort, n.d.), Ossim tiene una versión personalizada la cual nos da las alertas sobre los intrusos a nuestra red.

- **OpenVAS**: Escáner de vulnerabilidades, características incluyen pruebas no autenticadas, autenticadas, protocolos de internet de alto y bajo nivel, escaneos a gran escala (OpenVas, n.d.).

- **Ntop**: Herramienta Open Source para la monitorización del tráfico de la red en tiempo real, permite controlar el consumo de recursos por parte de los usuarios y aplicaciones que se usen a diario y detectar más las configuraciones de equipos (NTOP, n.d.).

- **Nagios**: Herramienta de monitorización de código abierto, censa dispositivos y servicios, alerta cuando existen anomalías en los mismo (Robiedo , 2011).

- **NMAP**: Escáner de red, herramienta que permite escanear puertos en dispositivos computacionales dentro de una red, identifica puertos abiertos, cerrados o protegidos, así como servicios utilizados por dispositivos incluyendo información sobre el Sistema Operativo.

2.7.2. OSSIM-SERVER

Como toda aplicación, AlienVault Ossim funciona con un estándar cliente servidor y es obligatorio tener un solo servidor en toda nuestra red en el cual al instalar el perfil server (servidor) estamos configurando el ambiente que se encargue de procesar y recoger todos los logs que son generados por los diferentes dispositivos y servidores de nuestra red interna (Rodriguez, 2016).

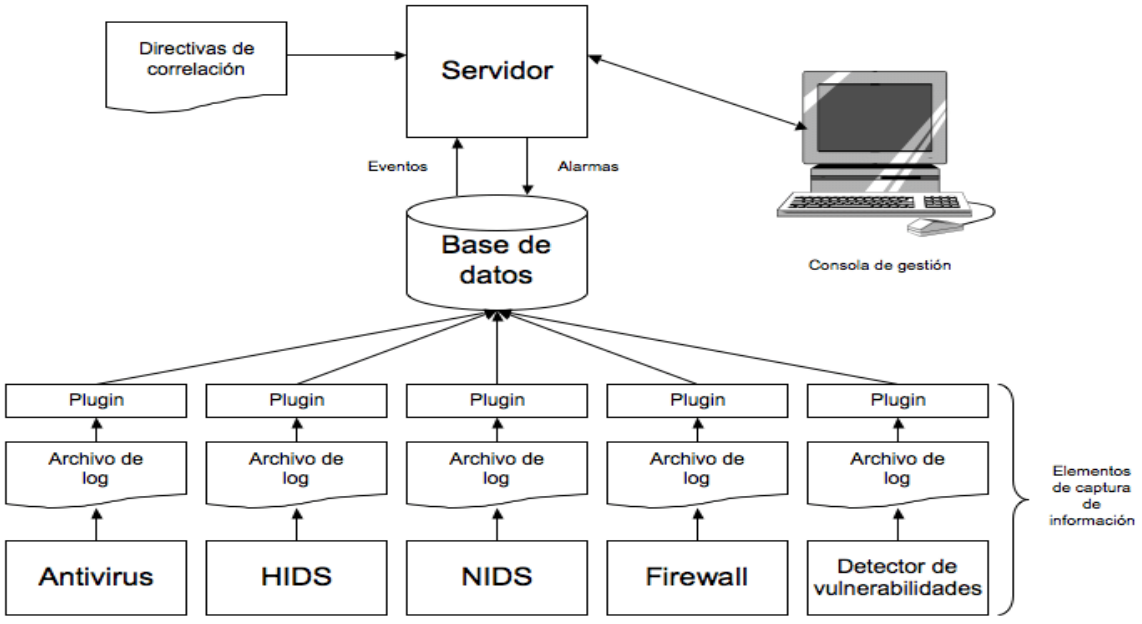


Figura 10 Arquitectura AlienVault Ossim.
Fuente : (Juan, Luis, Carlos, & Juan, 2008)

En la siguiente tabla se describen los puertos que AlienVault OSSIM utiliza para la comunicación.

Tabla 3 Tabla de puertos de comunicación

Puertos	Abierto	Servicios
40001-40002	X	CLOUD
3306	X	MYSQL
22	X	SSH
443	X	HTTPS
25	X	SMTP
80	X	HTTP
8080	X	HTTP-PROXY

Fuente: Autores

2.7.3. OSSIM FRAMEWORK

El propósito de AlienVault Ossim ha sido implantar un framework capaz de recoger toda la información de los diferentes complementos, para incorporar e interrelacionar entre sí, conseguir una visualización exclusiva del estado de la red, con el propósito de aumentar la detección de anomalías, priorizar los eventos del contexto que se producen y optimizar la visibilidad de la monitorización del estado de la red actual como se muestra en el diagrama de la figura 11 (Juan et al., 2008).

Diagrama de funcionamiento del Ossim-framework

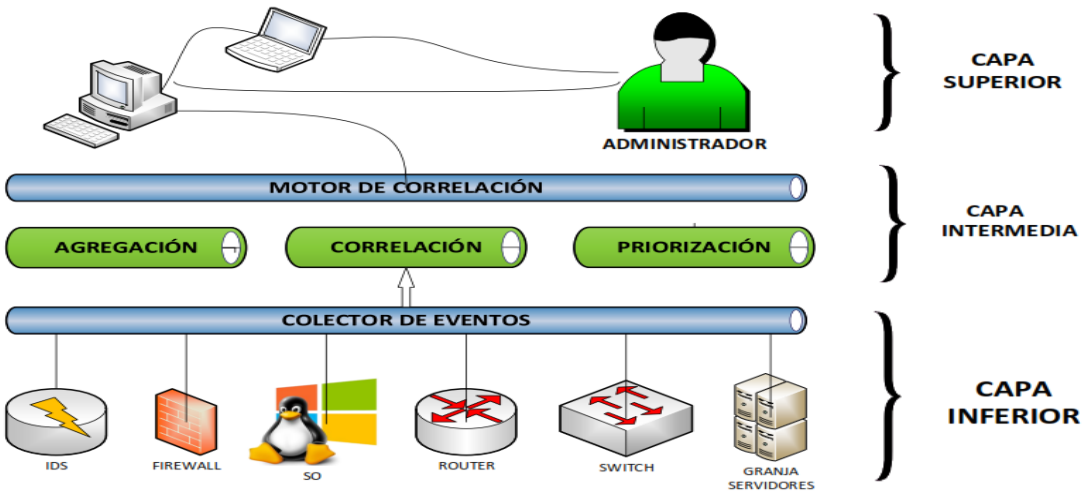


Figura 11 Diagrama de capas AlienVault Ossim
Fuente: Autores

En la ilustración anterior evidenciamos que OSSIM- FRAMEWORK interactúa entre la capa inferior e intermedia y así presentar la información al usuario a través de la interfaz web en la capa superior.

- Preprocesado (capa inferior): Capa más baja del OSSIM, donde se colectan los eventos, se componen de detectores, monitores, designados preprocesadores los cuales detectan y generan alarmas para luego enviar datos al sistema central para colectarlos y hacer el análisis de los eventos.
    - Sistema detector de intrusos (detecta patrones)
    - Detectores de anomalías
    - Firewalls
    - Monitores (plugins)

- Postprocesado (capa media): Interpreta eventos por agentes o sensor, traduciéndolos para ser interpretados por el administrador, relaciona la información colectada y proporciona un apunte legible a través de avisos o alertas.

- Front-end (capa superior): Interacción con la herramienta, visualiza eventos, configuración de la herramienta, administración del sistema, en ella podremos crear políticas de seguridad, definir reglas de correlación y enlazar las diferentes herramientas integradas.

2.7.4. PROCESO DE DETECCIÓN

El principal objetivo del proyecto AlienVault OSSIM, es aumentar la capacidad de detección que es ofrecida por productos hasta ahora desarrollados, el mismo consta de:

- **Detectores**, denominado a la aplicación que busca patrones en tiempo real produciendo eventos de seguridad. La capacidad de detección de un detector se defines por 2 sustantivos:

- Sensibilidad, capacidad de análisis y complejidad, que tiene el detector para ubicar una anomalía.
- Fiabilidad, nivel de convicción ofrecido por el detector frente a un posible ataque.

Los principales problemas de los detectores para afrontar la detección encontramos:

- Falsos Positivos, es la falta de fiabilidad en los detectores, posibles ataques que no corresponden con ataques reales.
- Falsos Negativos, la incapacidad de detección, los ataques pasarían por alto, “falta de sensibilidad”

- **Postproceso,** mecanismos para mejorar la sensibilidad y fiabilidad de la detención reduciendo falsos positivos.

2.7.5. OSSIM-AGENT

El nombre de Agent en la herramienta AlienVault Ossim se les da a los plugins y aplicaciones que permite analizar todos los eventos específicos que se generan en la red de trabajo o en los diferentes servidores en la cual se está haciendo el monitoreo y seguimiento (Rodriguez, 2016).

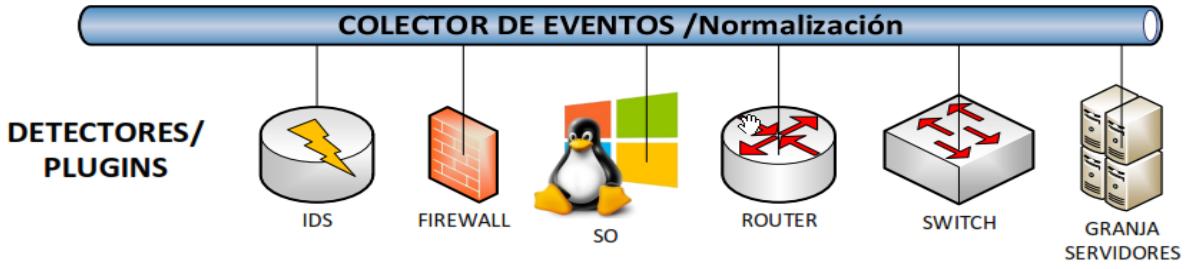


Figura 12 Ossim colector de eventos
Fuente: Autores

2.7.6. MODELO DE ARQUITECTURA OSSIM

En este modelo podemos diferenciar dos partes la primera distribuida y la segunda centralizada en las cuales se despliega los dos instantes diferentes de proceso:

- Preproceso
- Postproceso

La figura 13 se representa la función detallada de cada uno de los procesos.

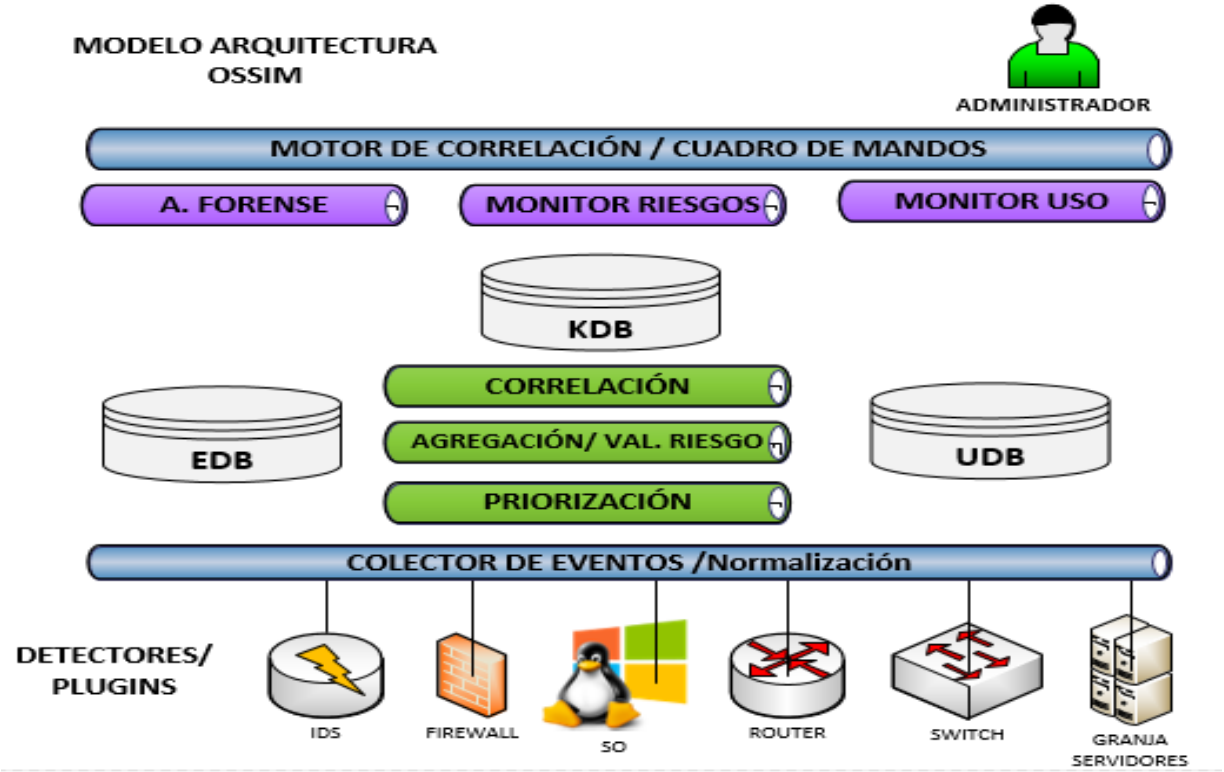


Figura 13 Modelo de Arquitectura Ossim
Fuente: Autores

Ossim utiliza 3 bases de datos diferentes para los diversos tipos de registros almacenados:

- EDB, base de datos eventos, la más grande guarda todos los eventos recibidos de detectores.
- KDB, base de datos Framework, guarda datos sobre red y definición de políticas de seguridad.

- UDB, base de datos perfiles, almacena información aprendida por el monitor de perfiles.

Con la implementación del presente trabajo se ejecutan herramientas preparadas para escuchar el tráfico de red, búsqueda de esquemas malignos determinados a partir de reglas o políticas, los mismos provocan eventos de seguridad, los más frecuentes IDS, NGFW o cualquier otro componente de red como router, switch o los mismos sistemas operativos, esto con el objetivo de descubrir esquemas en la red entre estos escanear puertos, spoofing, ataques por fragmentación, los mismos tienen sus propios eventos de seguridad, capaces de alertar de posibles incidencias en la red, los cuales podemos coleccionar para su posterior análisis en los motores de correlación.

El sistema de colección es el encargado de unificar todos los logs de seguridad en una única consola y formato, todos estos eventos son almacenados en la EDB (Base de Datos Eventos), haciendo posible observar en una sola pantalla y tamaño los eventos de seguridad en un lapso de tiempo, ya sean del router, FW, IDS, o cualquier SO.

La prioridad determinada para una alerta dependerá de la infraestructura de red, registros de cada dispositivo y el rol que desempeña en la institución, el mismo que será almacenado en una dase de conocimientos formada por: Inventario de equipos y dispositivos de red (ip, mac, SO, servicios, etc.) y las Políticas de accesos. Estas medidas son almacenadas en la base de datos KDB, de esta manera el sistema conocerá la topología de red, características de los dispositivos y las políticas de seguridad determinadas.

Los monitores de la red hacen posible la detección de eventos cuando estos ocurran pues detectarán la actividad anómala, los monitores de perfiles ofrecen datos específicos sobre el uso realizado por el usuario permitiendo establecer un perfil por ejemplo, uso de correo, pop, http, estos datos se obtienen de la base de datos de perfiles UDB.

Mediante el uso de la consola web permitirá el acceso a información almacenada en la EDB, permitiendo analizar de manera centralizada los eventos de seguridad y los elementos críticos de la red, desplegando una Ciberseguridad en profundidad sobre cada uno de los eventos ocurridos en el sistema.

CAPÍTULO III. DESARROLLO METODOLÓGICO

3.1. TIPO Y DISEÑO DE LA INVESTIGACIÓN

Debido a que el objeto de estudio es diseñar un plan de fortalecimiento ante ataques informáticos del Hospital de Especialidades Portoviejo basados en sistemas de correlación de log, el tipo de investigación que se uso es cuasi experimental con un enfoque cualitativo, el cual permitió analizar la información y encontrar una solución al problema planteado, partiendo de los resultados de la misma, de acuerdo a Fidias (2017) “La investigación experimental es un proceso que consiste en someter a un objeto o grupo de individuos en determinadas condiciones, estímulos o tratamiento (variable independiente), para observar los efectos o reacciones que se producen (variable dependiente)”.

3.2. METODOLOGÍA PPDIOO

Se utilizó la metodología PPDIOO (Preparar, Planear, Diseño, Implementación, Operación, Optimización) la misma que considera los pasos para la obtención de requerimientos, como se presentan en la figura 14.

Figura 14 Metodología PPDIOO
Fuente: Autores

3.2.1. FASE DE PREPARACIÓN

Esta fase consistió en investigar y evaluar las diferentes herramientas de Ciberseguridad que se encuentran disponibles en el mercado, tanto privado como libre con la finalidad de minimizar costos de implementación y despliegue al momento de hardenizar los sistemas que formaran parte de la seguridad centralizada, por lo que el despliegue de toda esta infraestructura será a nivel de IAAS (Infraestructura como servicio). Además, en esta fase se identifican las partes más importantes para la elaboración de la arquitectura en un laboratorio controlado.

Tabla 4 Componentes de una infraestructura de red

Infraestructura de red
a. Almacenamiento
b. Plataforma IAAS
c. Servicios (Base Datos, Correos, FW, IDS, IPS, Herramienta de monitorización, Seguridad, Sistema de correlación)
d. Seguridad Centralizada (Hardenización, criptografías, Esteganografía, herramientas de correlación anómalos WAF)

Fuente: Autores

3.2.2. FASE DE PLANIFICACIÓN

Para el presente proyecto fue necesario el cumplimiento de los siguientes requerimientos descritos en la siguiente tabla.

Tabla 5 Equipamiento necesario en el despliegue del laboratorio controlado

No.	**Requerimiento**
Almacenamiento	

1	S.O. libre para almacenamiento remoto en una red utilizando NAS.
2	Adaptable a cualquier ordenador para reducir costos y aumentar la flexibilidad.
Plataforma y Servicios	
6	Infraestructura robusta y tolerante a fallos.
7	Plataforma de virtualización.
8	Sistemas virtuales independientes
Seguridad	
9	Sistema de gestión de la información de seguridad.
10	Integración de sistemas de monitorización y detección de patrones de datos
11	Implementación de data store “plugins” para integrar e interrelacionar los componentes de la seguridad centralizada.
12	Gestionar políticas de seguridad y definir nuevas reglas de correlación de eventos anómalos.

Fuente: Autores

3.2.3. FASE DE DISEÑO

En esta fase se tomó como referencia el diseño de la red de datos del HEP y se propuso un nuevo diseño incorporando mecanismos de Ciberseguridad basados en correlación de eventos, se adjunta en la figura 15 el diagrama actual de la red del HEP.

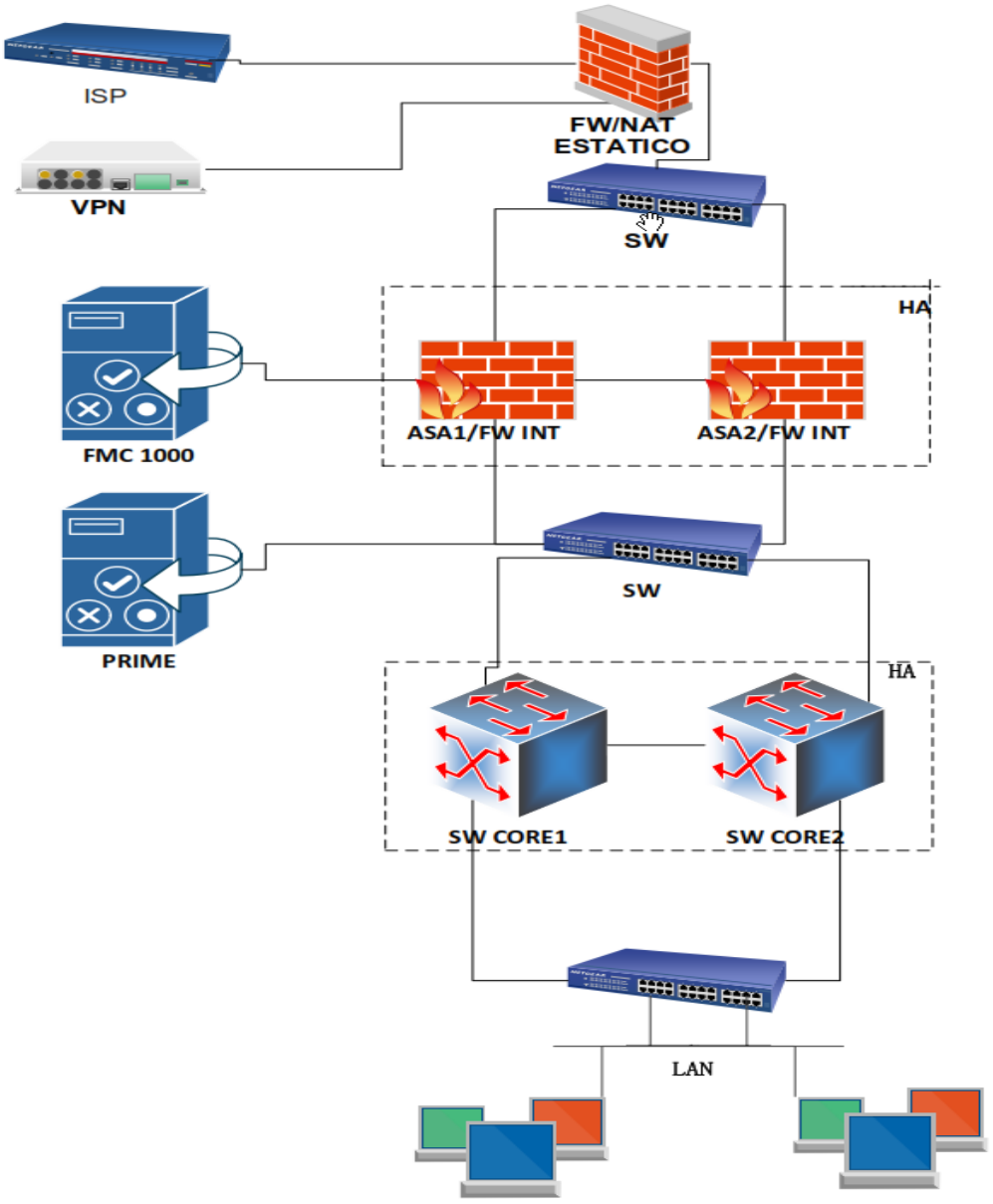


Figura 15 Diagrama de Red Hospital de Especialidades
Fuente: Autores

Según el diagrama de red actual del Hospital de Especialidades Portoviejo, el mismo es un modelo de red de núcleo colapsado, en el cual se tienen varias capas para la interconexión y comunicación de los dispositivos de red, pero existe una gran deficiencia en cuanto al control y seguridad de la red, pues muchos de sus sistemas aunque sean robustos en su accionar existe la falencia del licenciamiento para

poder funcionar al 100% o poder explotar totalmente sus características tecnológicas.

Además de lo mencionado, el FW (Firewall) como los IDS (Sistema Detección de Intrusos), y los dispositivos de red generan logs, que son tratados independientemente por cada equipo, en ciertos casos incluso dichos logs no son tomados en cuenta y no existe un tratamiento de dicha información, provocando un desconocimiento en el personal de TICs del Hospital de Especialidades Portoviejo en cuanto a la existencia o no de posibles ciberataques en tiempo real, así como no contar con una herramienta o cuadro de mando que permita tomar decisiones o realizar políticas de mejoras en ciberdefensa.

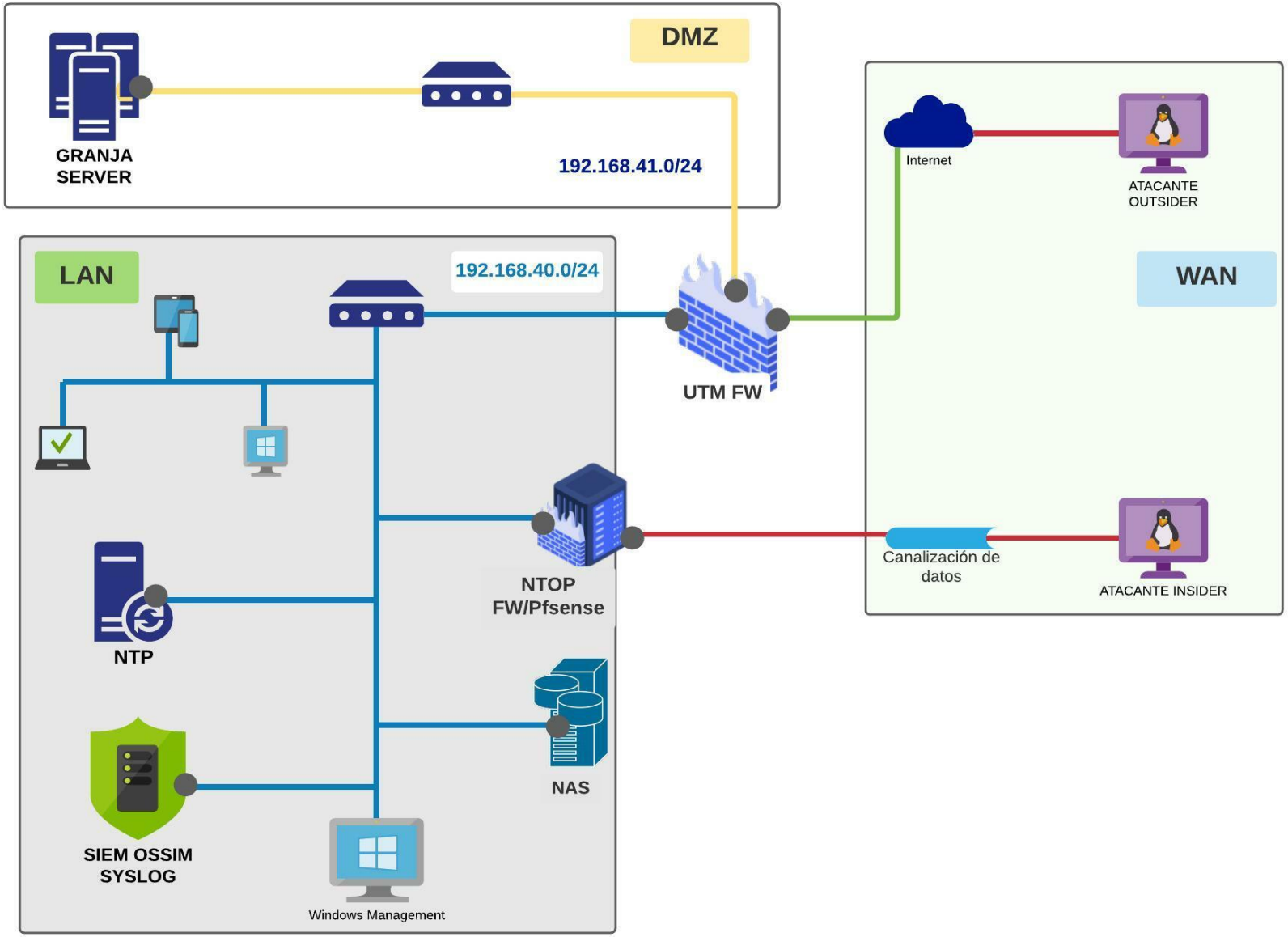


Figura 16. Diagrama del laboratorio de pruebas propuesto
Fuente: Autores

En el diagrama propuesto para esta investigación se presenta un nuevo esquema de red, en la que todos los elementos que intervienen trabajen de manera síncrona, permitiendo colectar los eventos que ocurren en la red del HEP, la cual está basada en un sistema de correlación de eventos, de esta manera los diferentes eventos pueden ser tratados y permitir a los sistemas de monitorización analizar los paquetes entrantes y salientes, toda esta información será analizada con la herramienta AlienVault OSSIM, que permitirá tener una defensa en profundidad con la cual se aplicaron controles de seguridad para proteger los datos en diferentes capas.

Para la ejecución y cumplimiento de los preceptos de esta investigación se propuso el siguiente diagrama de red, se muestra en la figura 16, asimismo en la siguiente tabla tenemos el direccionamiento IP usado en la topología propuesta.

Tabla 6. Direccionamiento IP

HERRAMIENTA	DIRECCION IP	Gw	TYPO	DESCRIPCION
PFSENSE	192.168.40.1/24	192.168.40.81	Dispositivo de red	Internet
	192.168.41.8/24			Zona desmilitarizada
MONOWALL	192.168.40.81/24		Linux	Zona desmilitarizada
	OPT			Internet
	192.168.41.1/24			Red LAN
IPCOP / NTP	192.168.40.233/24	192.168.40.81	Dispositivo de red	Hora del Sistema
OSSIM	192.168.40.209/24	192.168.40.81	Linux	Gestión
	192.168.40.210/24			Sensor

FREENAS	192.168.40.40/24	192.168.40.81	Dispositivo de red	Almacenamiento red
WINDOWS 7	192.168.40.123/24	192.168.40.81	Windows	Pc gestión
WINDOWS SERVER	192.168.41.159/24	192.168.41.1	Windows	PC
PC ATACANTE	192.168.41.99/24	192.168.41.1	Kali Linux	Insider

Fuente: Autores

3.2.4. FASE DE IMPLEMENTACIÓN

Al establecer los parámetros de diseño y lineamientos se procedió con la ejecución del laboratorio de pruebas, como herramienta base para la implementación del laboratorio se ejecutó la instalación del sistema de virtualización, dentro de la misma se instaló y configuro las siguientes máquinas virtuales y físicas para lograr los objetivos de la presente investigación, cabe mencionar que todos los sistemas operativos y herramientas utilizadas en la presente investigación es de carácter de libre distribución a excepción de las máquinas virtuales de prueba windows:

Tabla 7. Máquinas Virtuales y Herramientas Utilizadas

MAQUINAS VIRTUAL	HERRAMIENTAS
Kali Linux	NMAP
Windows Server	Metasploit Framework
Windows cliente (Windows 7)	Openvas
Firewall IPCOP	Nagios
Firewall PFSENSE	La Hidra
Firewall MONOWALL	

FREENAS
AlienVault OSSIM

Fuente: Autores

3.2.5. FASE DE OPERACIÓN

Las amenazas cibernéticas evolucionan y se vuelven cada vez más maliciosas, así también evoluciona la ciberseguridad, de este modo surge la Defensa en Profundidad (Defense in Depth DID). DiD es una técnica de ciberseguridad que hace uso de diferentes medidas de seguridad para proteger la integridad de la información, esta defensa se basa en la seguridad por capas la cual tiene su origen en una estrategia militar que consistía en colocar diferentes barreras para frenar el avance enemigo (Guijarro, Yepez, Peralta, & Ortiz, 2018). La arquitectura de la seguridad en capas consiste en:

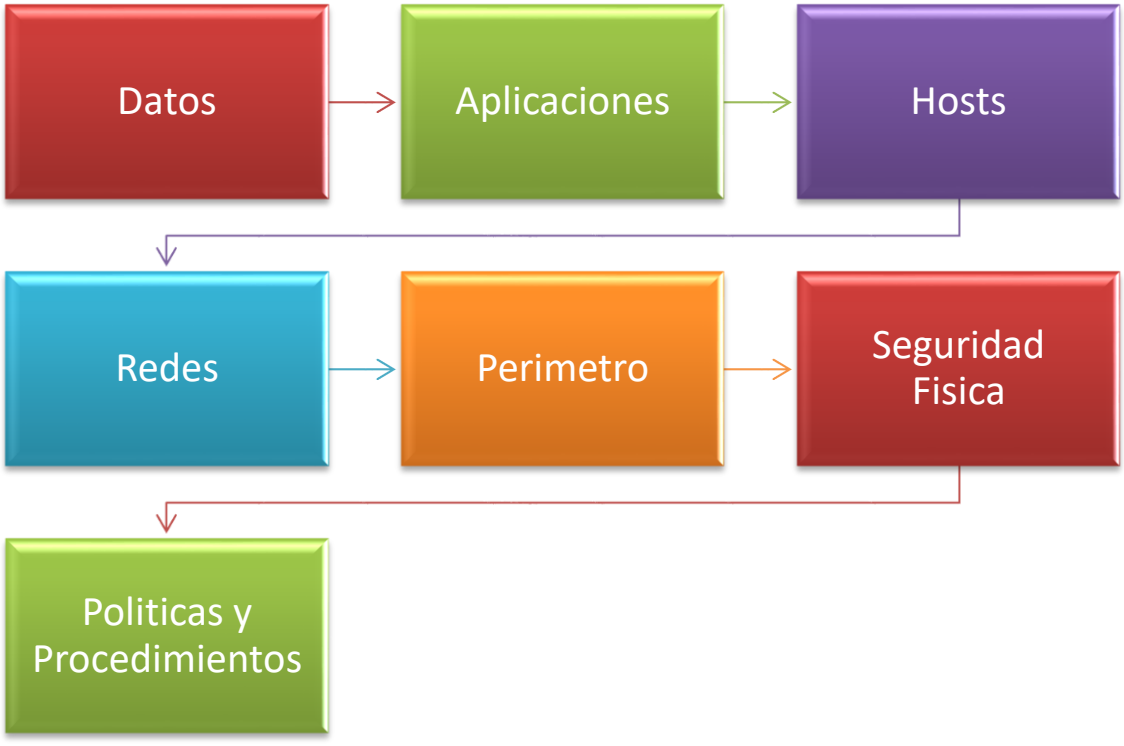


Ilustración 1 Capas de seguridad Defensa en Profundidad
Fuente: Autores

En esta fase se puntualiza el análisis funcional del laboratorio de pruebas realizado en base a las exigencias. Al definir las interfaces y su tipo, podremos realizar escaneos pasivos de la red. Identificando dispositivos computaciones y equipos de red que van a ser monitoreados a través de la herramienta.

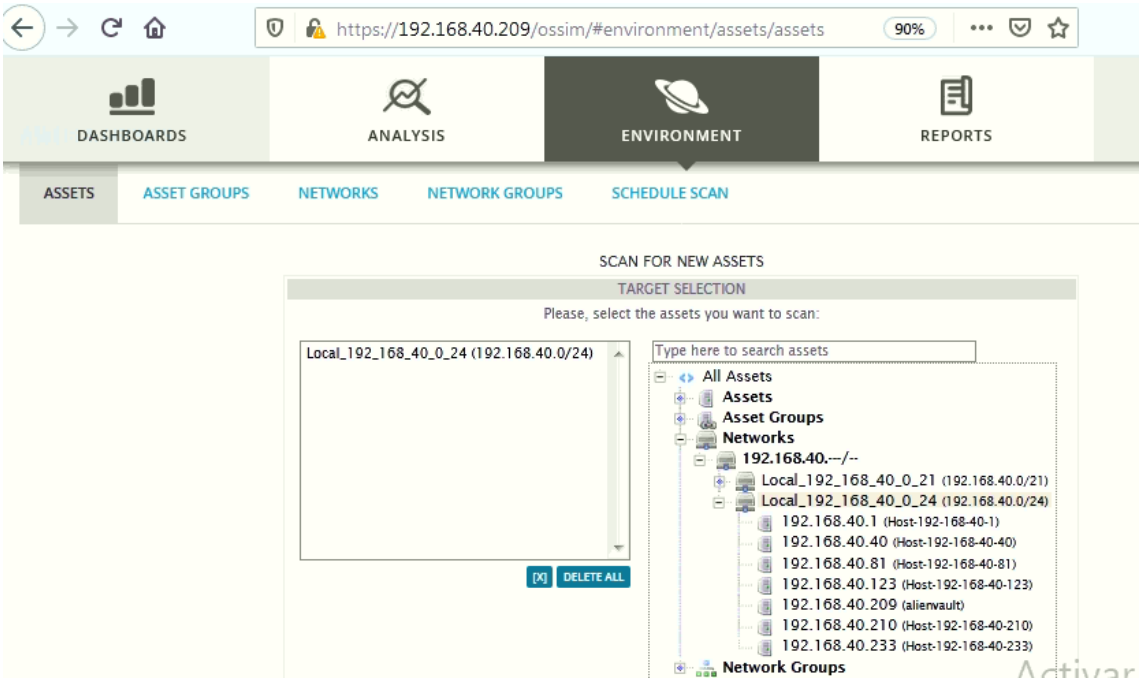


Figura 17. Descubrimiento de estaciones de trabajo o redes
Fuente: Autores

3.2.6. FASE DE OPTIMIZACIÓN

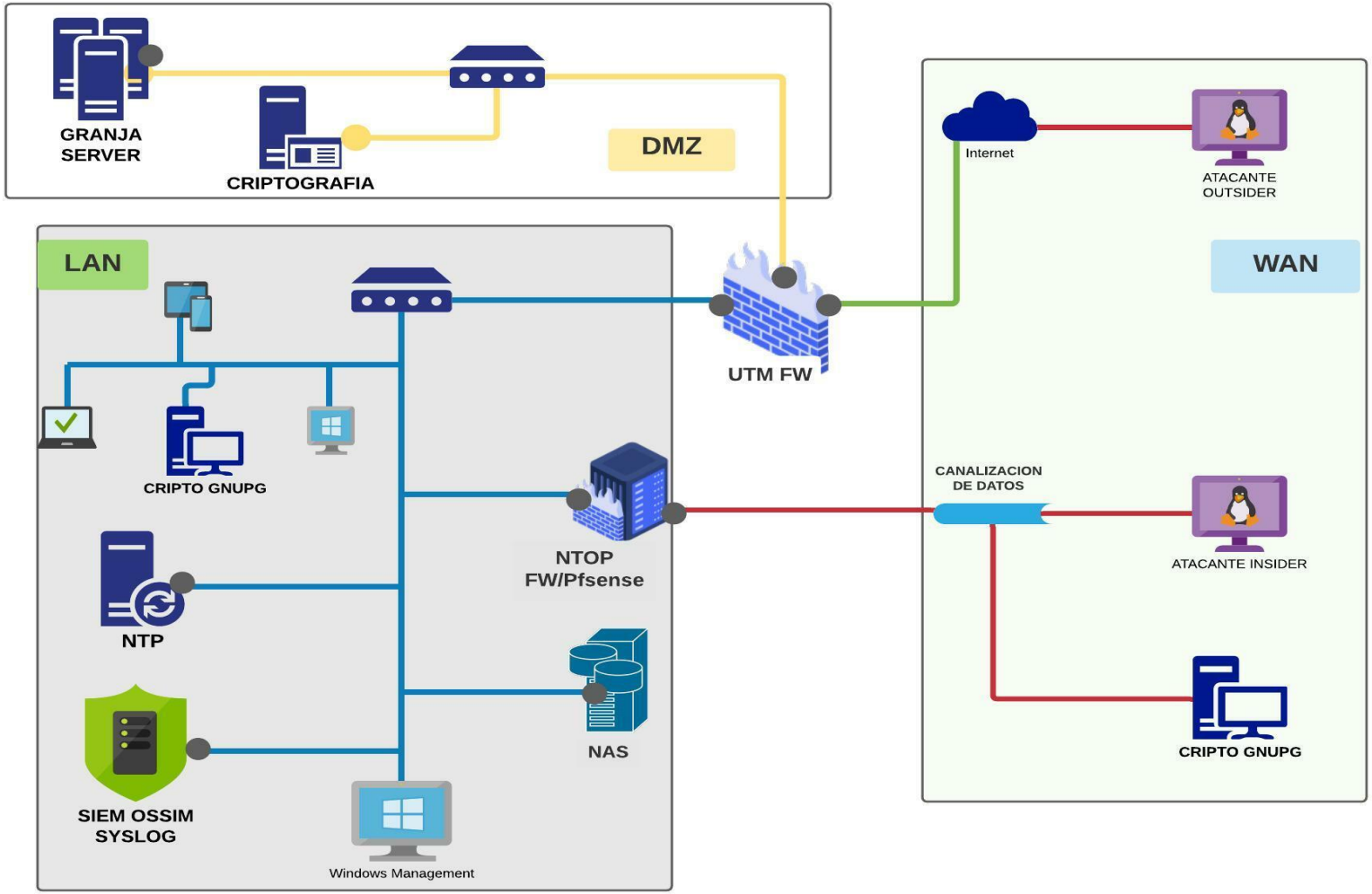


Figura 18 Diagrama de red optimizado
Fuente: Autores

En la fase de optimización como aporte para la infraestructura se propuso, agregar al diseño de red una herramienta de criptografía asimétrica, la cual nos permite establecer conexiones seguras entre dos partes autenticando mutuamente a las partes y permitiendo el traspaso de información entre los dos, esto con la unificación de todas estas herramientas tecnológicas permitió la optimización de una seguridad centralizada basado en sistema de correlación de logs (Cordova, Vega, Rodriguez, & Escobedo, 2020).

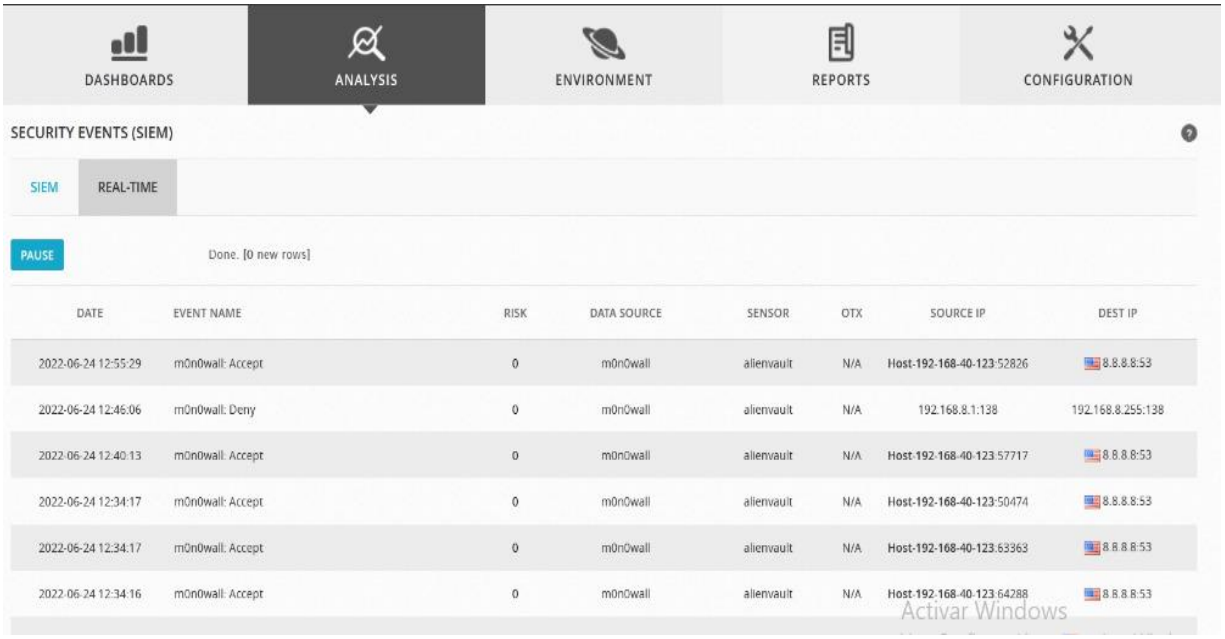


Figura 19 Logs Generados en Tiempo Real
Fuente: Autores

En la imagen 19 se visualiza una muestra de los logs que fueron detectados por el AlienVault OSSIM en tiempo real, donde se encuentran logs generados por el Monowall teniendo varios en una hora determinada.

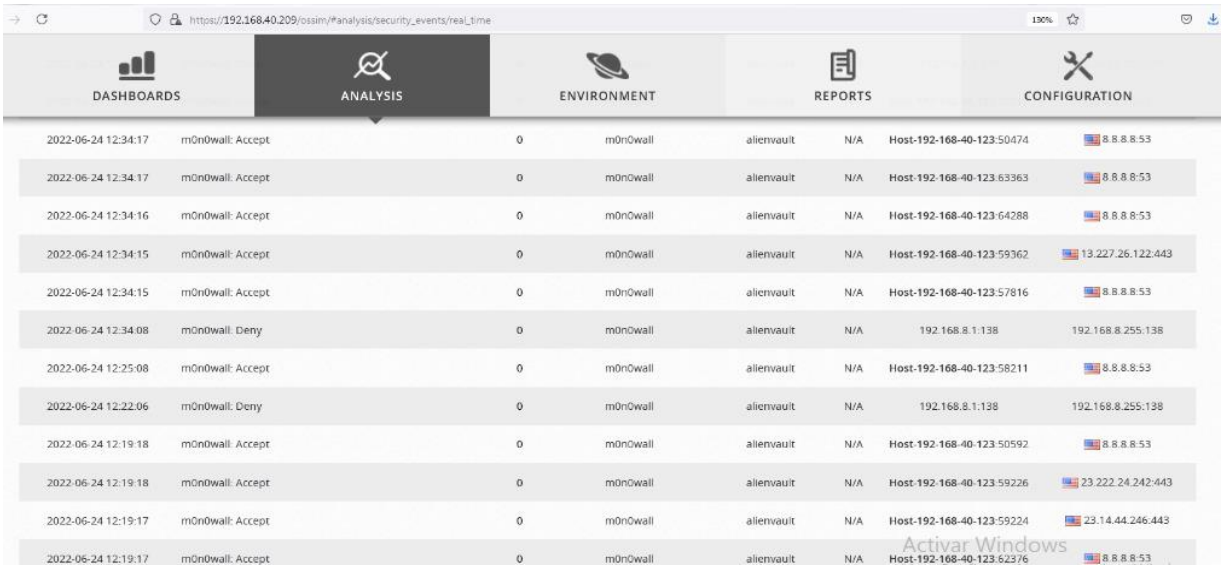


Figura 20 Logs Generados
Fuente: Autores

Se puede observar en la figura 20 los logs generados que están siendo detectados por la herramienta AlienVault OSSIM, se muestra el evento si es aceptado o denegado, la raíz del evento, la IP origen y el tiempo en el cual se ejecutó determinado evento.

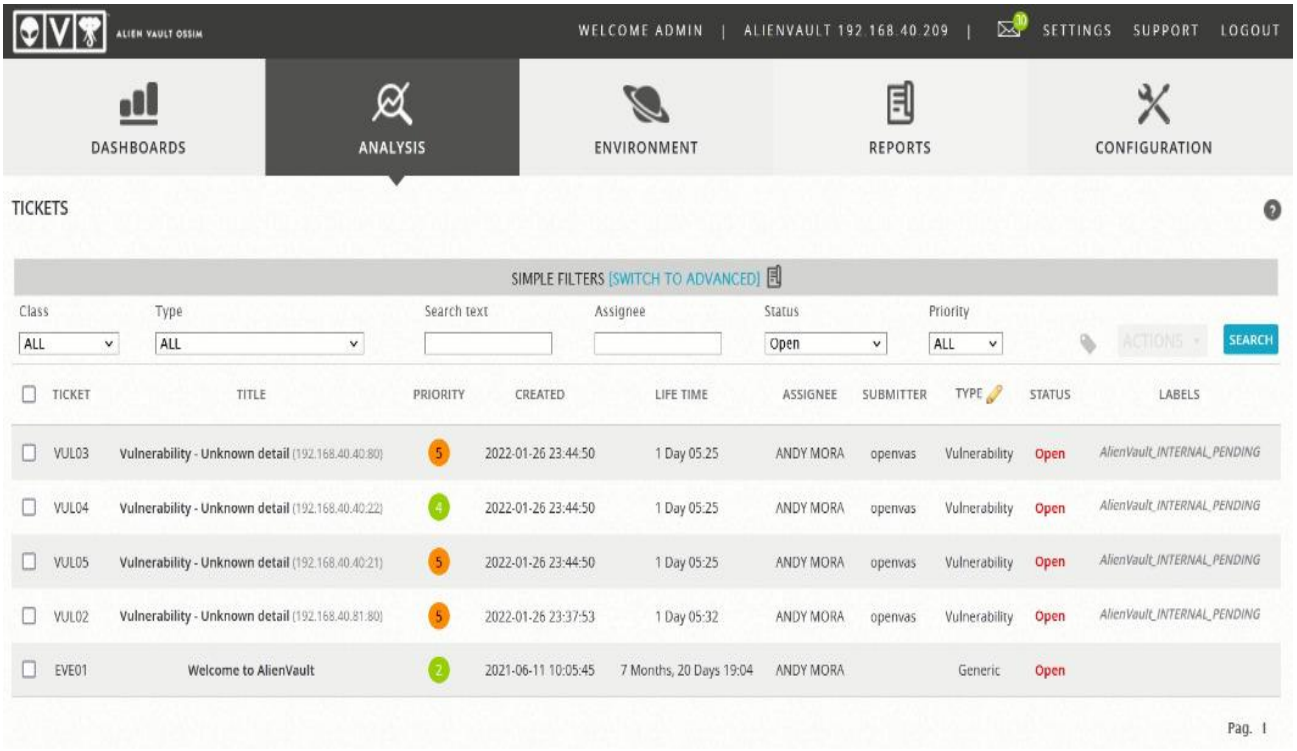


Figura 21. Ticket generado por análisis de vulnerabilidades
Fuente: Autores

Se observa en la figura 21 los tickets generados por vulnerabilidad donde tenemos el tipo de ticket, la prioridad, el estado en el que se encuentra que está abierto, el tiempo de vida que han tenido.

Figura 22. Detalle de Ticket
Fuente: Autores

Detalle del ticket presenta el estado, prioridad, la IP del equipo en este caso es la 192.168.40.81 que corresponde al Monowall y la solución es actualizar a versión señalada o posterior.

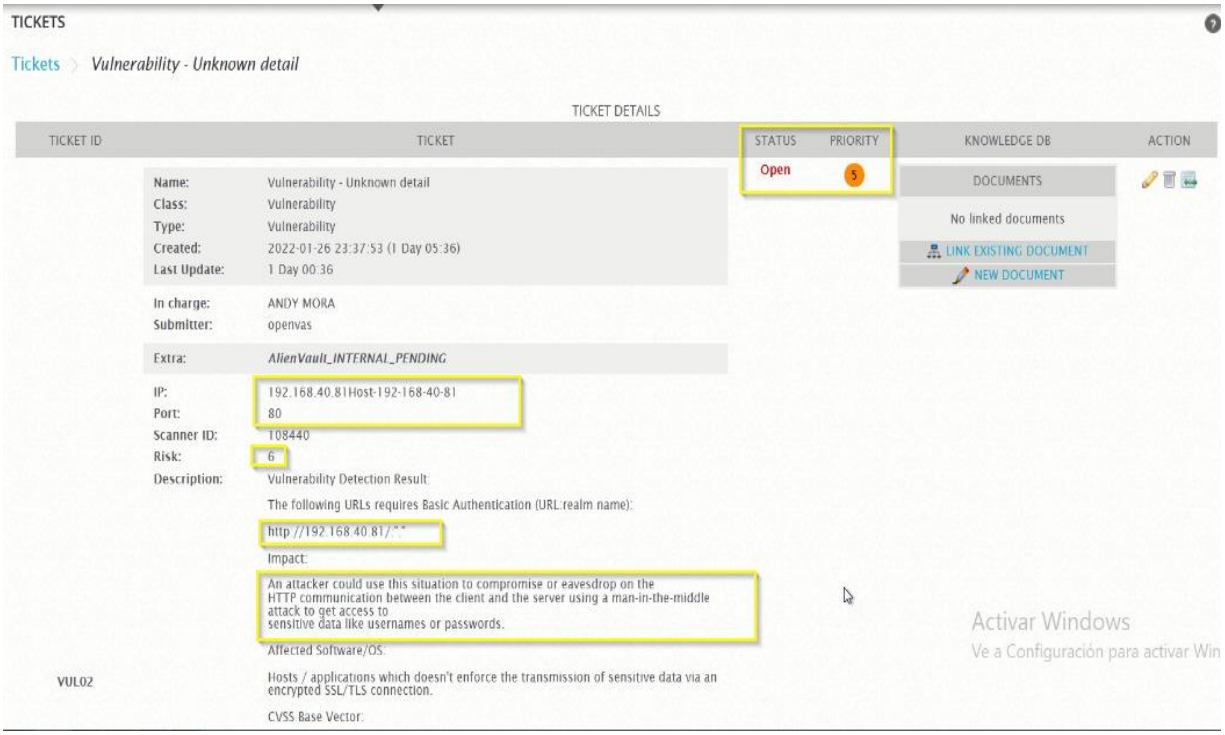


Figura 23. Detalle ticket Monowall
Fuente: Autores

En la figura 23 se observa un ticket para Monowall nos señala que existe la vulnerabilidad en el protocolo http en la manera como se autentica, el impacto de esta situación es que puede existir un ataque de hombre en el medio (Man in the middle) el ataque puede acceder a los username o password.

Figura 24. Detalle Ticket
Fuente: Autores

En la figura 24 el detalle del ticket del equipo FreeNas con IP 192.168.40.40 el cual tiene abierto el puerto 21 FTP como se observa.

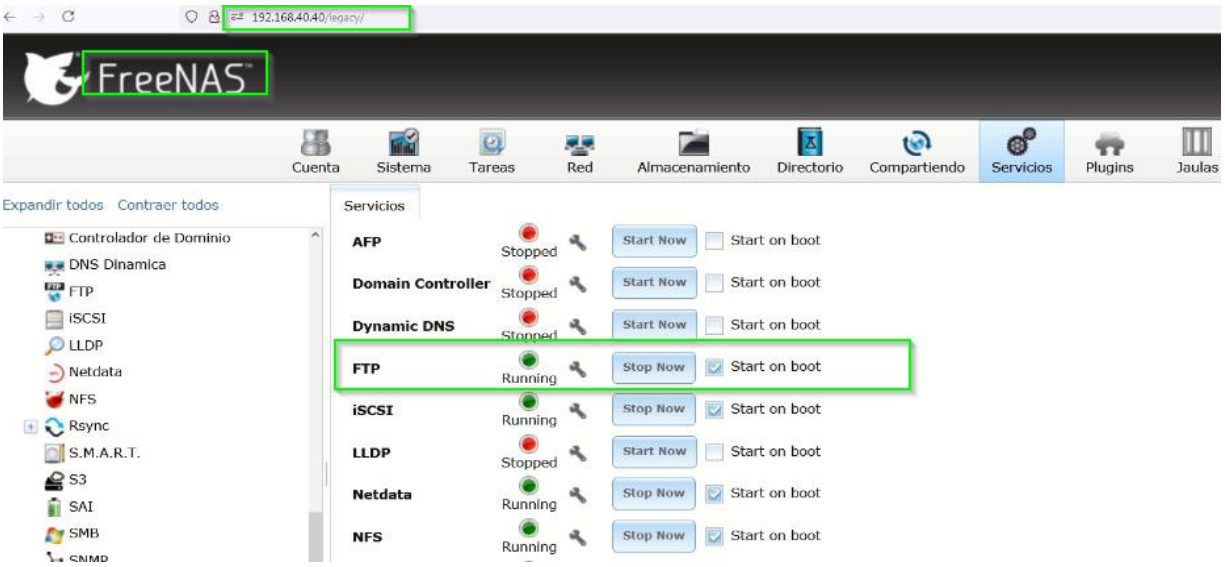


Figura 25. Verificación Puerto FreeNas
Fuente: Autores

Verificamos y efectivamente el FreeNas 192.168.40.40, tiene activo el servicio FTP.

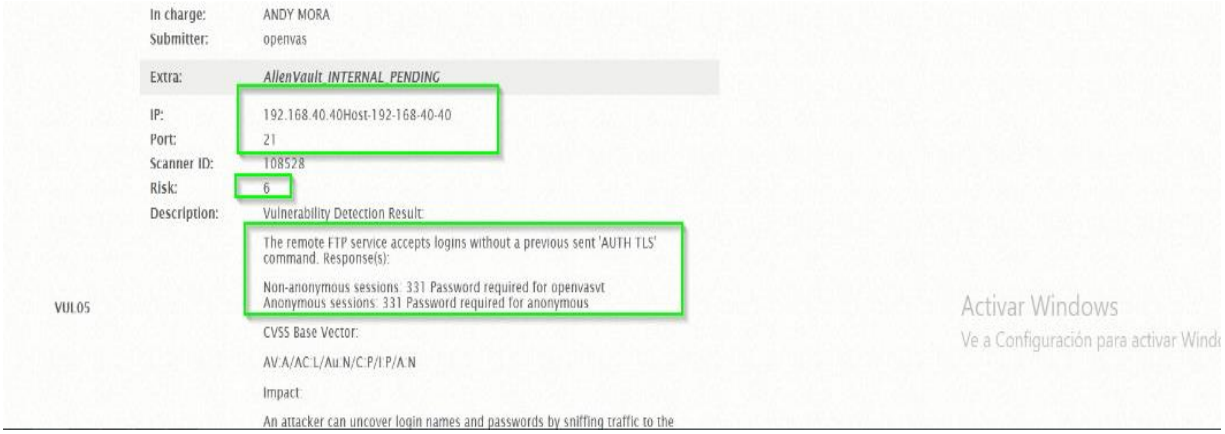


Figura 26. Posibles soluciones
Fuente: Autores

Como se observa en la figura 26 el ticket nos da posibles soluciones para solventar el problema que está suscitando nuestro equipo FreeNas y nos indica que debemos mejorar la configuración del servicio FTP o bloquear el mismo.

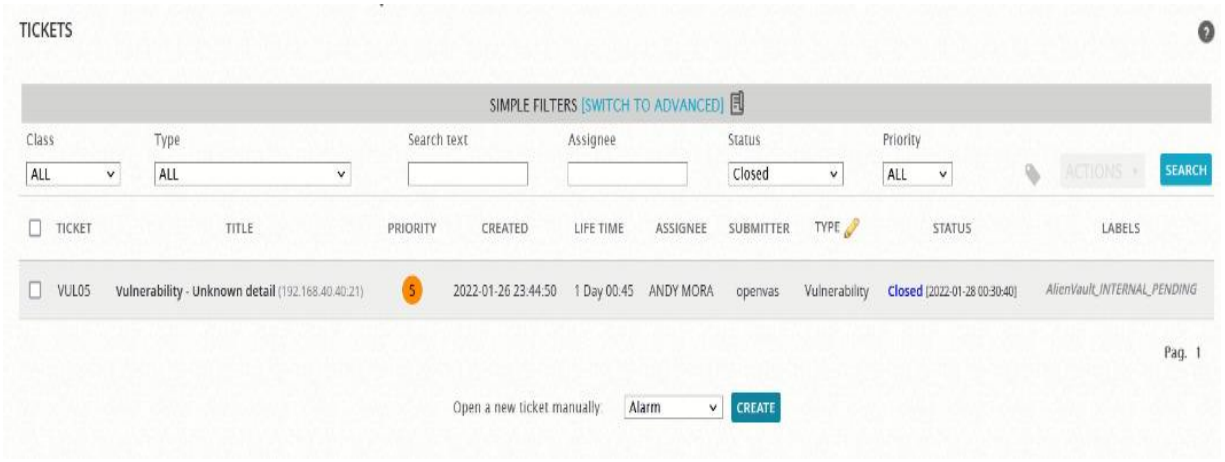


Figura 27. Ticket con estado cerrado
Fuente: Autores

Se realizó un filtro y se verificó el ticket con estado cerrado (closed) donde se muestra una vulnerabilidad con prioridad 5.

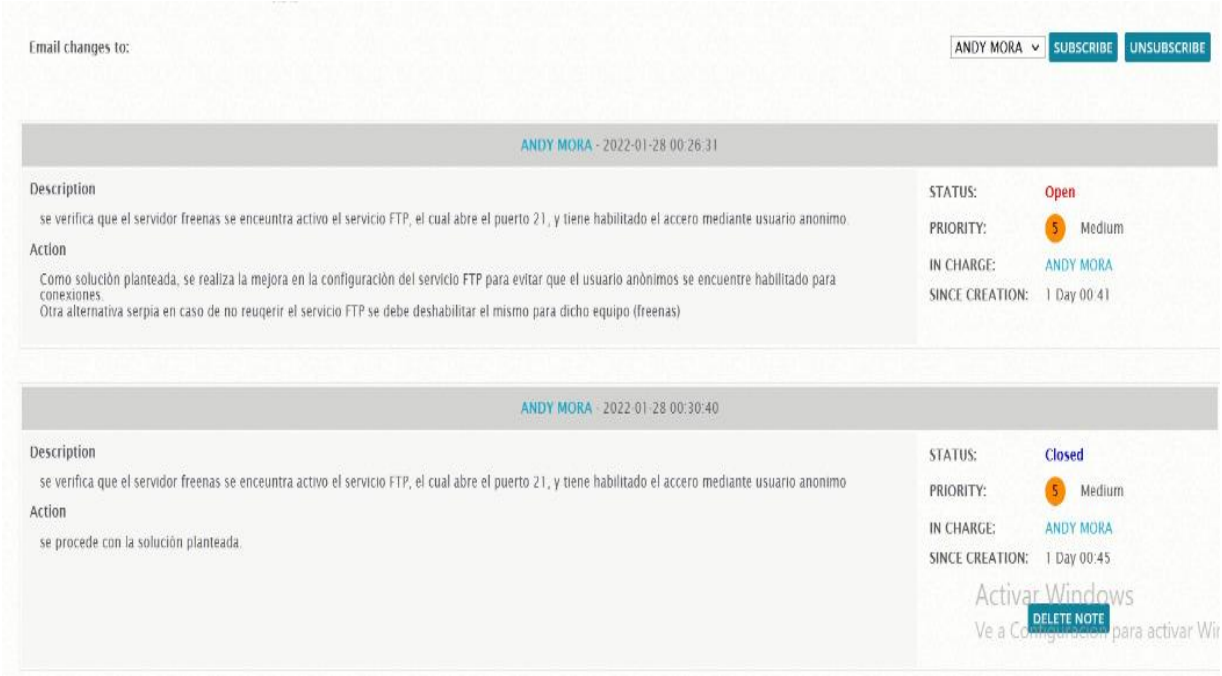


Figura 28. Descripción solución ticket
Fuente: Autores

Se visualiza en la figura los dos estados del ticket, cuando estaba abierto y su posible solución y una vez ejecutada la misma se muestra el estado actual del ticket y que ya se ha realizado la solución planteada correctamente.

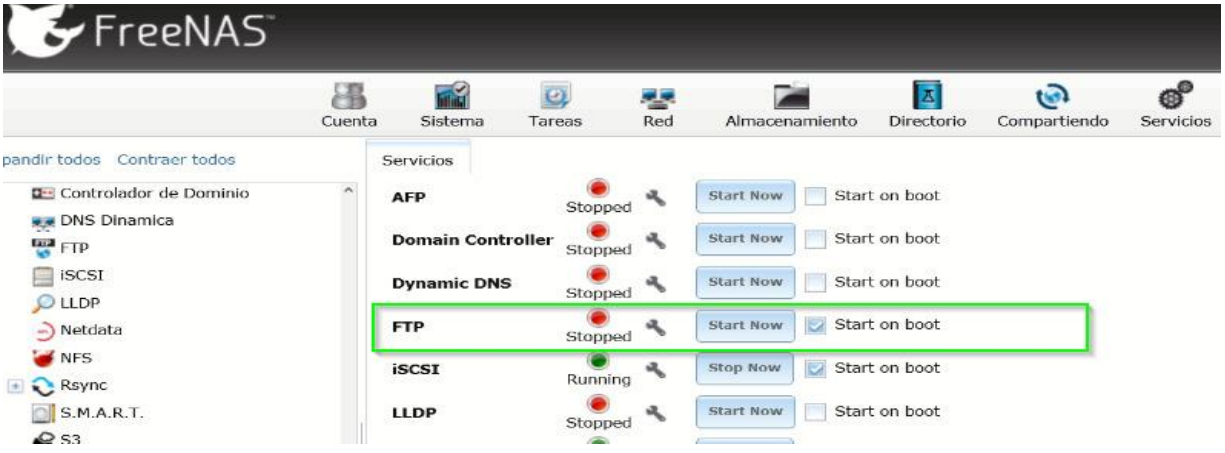


Figura 29. Revisión de solución FreeNas
Fuente: Autores

Una vez aplicada la solución planteada en el ticket se procede a revisar en el equipo FreeNas y se observa que el puerto FTP ya se encuentra cerrado como se visualiza en la figura 29, lo que indica que la anomalía está resuelta.

3.3. UBICACIÓN

Figura 30. Ubicación Hospital de Especialidades Portoviejo
Fuente: Autores

El trabajo de investigación se llevó a cabo en el Centro de Datos del Hospital de Especialidades Portoviejo (HEP), ubicado en la ciudad de Portoviejo provincia de Manabí en la avenida 15 de abril sector Tres Marías.

3.4. MÉTODO

En la realización de este proyecto para realizar la investigación se utilizaron los siguientes métodos:

3.4.1. MÉTODO ANALÍTICO

Se realizó un análisis de los eventos y logs obtenidos en los diferentes dispositivos que conformar la infraestructura de red del Hospital de Especialidades Portoviejo, mediante esto se evaluó varios factores como la cantidad de intentos de vulneración, posibles ataques y prevención de los mismos entre otros.

3.4.2. MÉTODO CUASI-EXPERIMENTAL.

Este método se utilizó para realizar las pruebas de ciberataques y ciberdefensa en base a los escenarios prácticos que se realizaron con los sistemas de correlación de logs, el cual sirvió para realizar un análisis de los resultados que se obtuvieron.

3.4.3. MÉTODO INDUCTIVO.

El método inductivo permitió la obtención de los conocimientos más básicos del funcionamiento de los sistemas de correlación de logs hasta comprender de manera general sobre este tema y poder desarrollar un plan de fortalecimiento ante ataques informáticos.

3.5. INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Se utilizaron los siguientes instrumentos de recolección de información:

3.5.1. TÉCNICAS

- Observación
- Entrevista

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Mediante los resultados obtenidos siguiendo los diferentes objetivos que se plasmaron y establecieron en esta investigación, se presenta el despliegue de las herramientas de seguridad centralizada basada en correlación de logs.

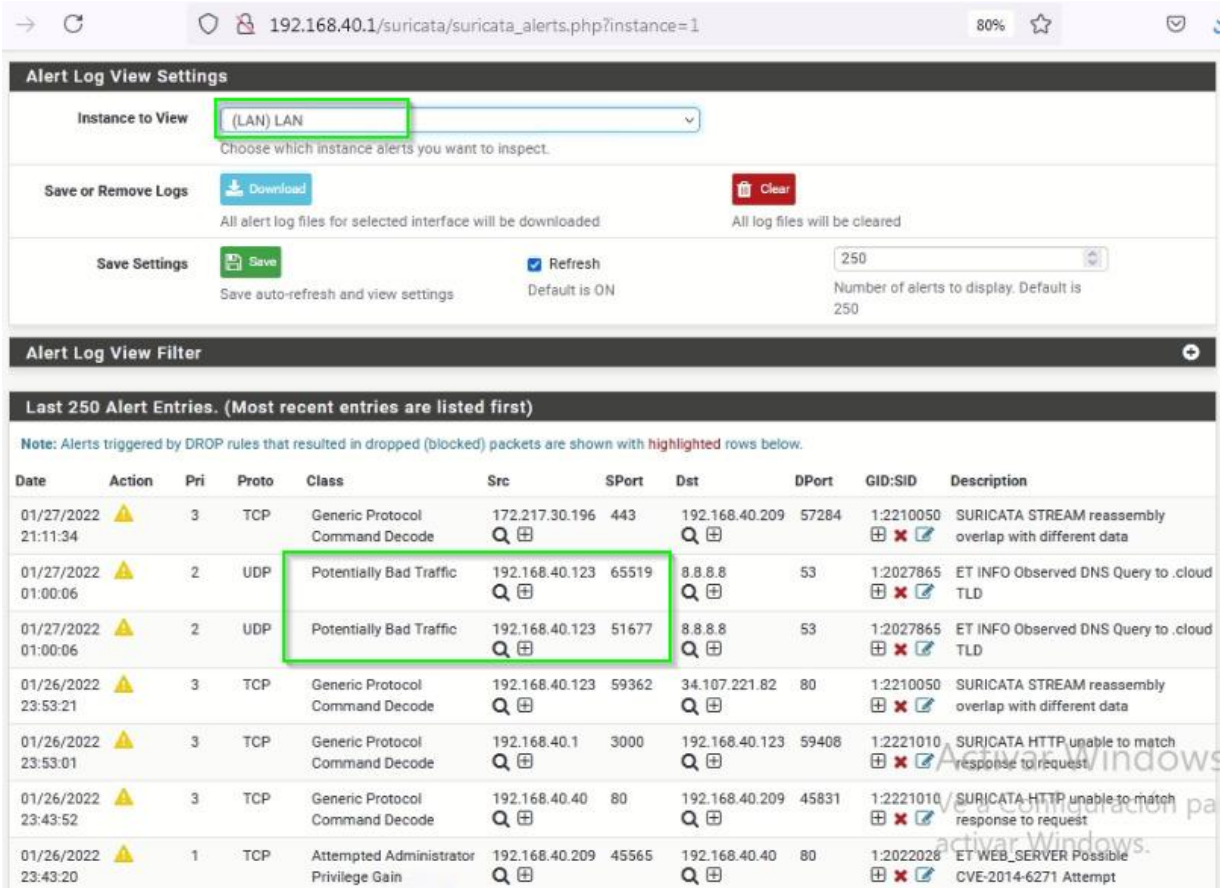


Figura 31 IDS posible tráfico anómalo
Fuente: Autores

En la figura 31 se puede observar ciertas anomalías en el tráfico de la red LAN, se encuentra el protocolo usado, la IP de origen siendo esta la 192.168.40.123, el puerto usado, la prioridad de la amenaza, descripción donde se muestra que es un DNS Query.

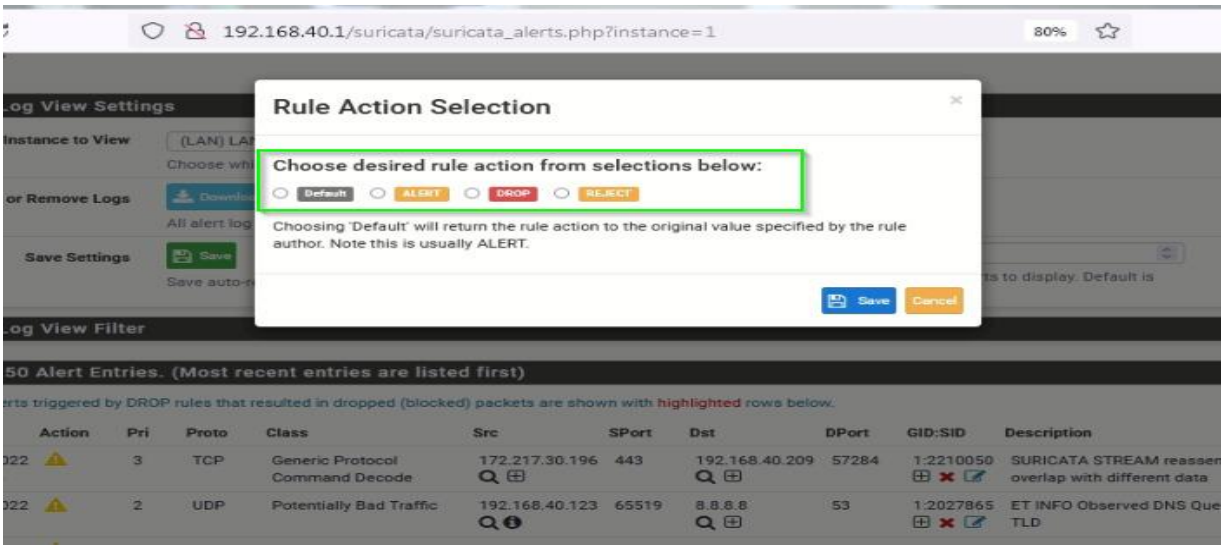


Figura 32. IPS selección de la acción a usar
Fuente: Autores

Asimismo, se observa en la figura 32 la regla o la acción a seleccionar para una determinada anomalía detectada por la herramienta entre los que procede: enviar un Alert, hacer un rechazo seleccionando Reject, no permitir con el Drop, y ponerla por defecto con el Default.

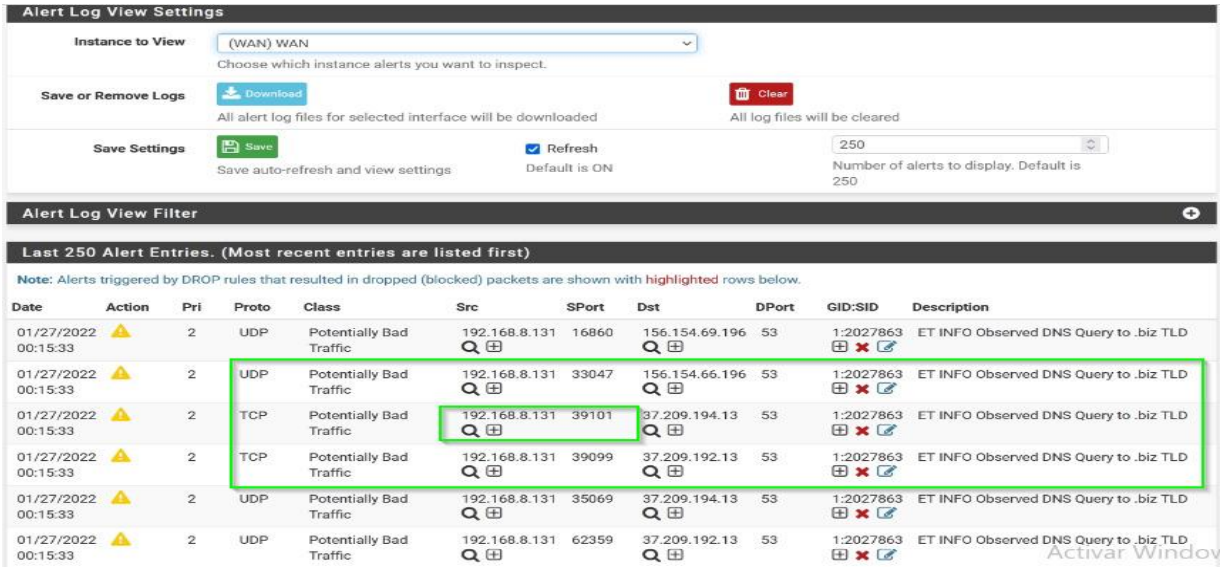


Figura 33. Trafico anómalo detectado por la WAN del Monowall
Fuente: Autores

La figura 33, muestra un tráfico anómalo detectado en la WAN del Monowall, en el cual, asumimos un tráfico por UDP y TCP con la IP origen 192.168.8.131 y la IP destino 37.209.194.13 en el puerto 53.

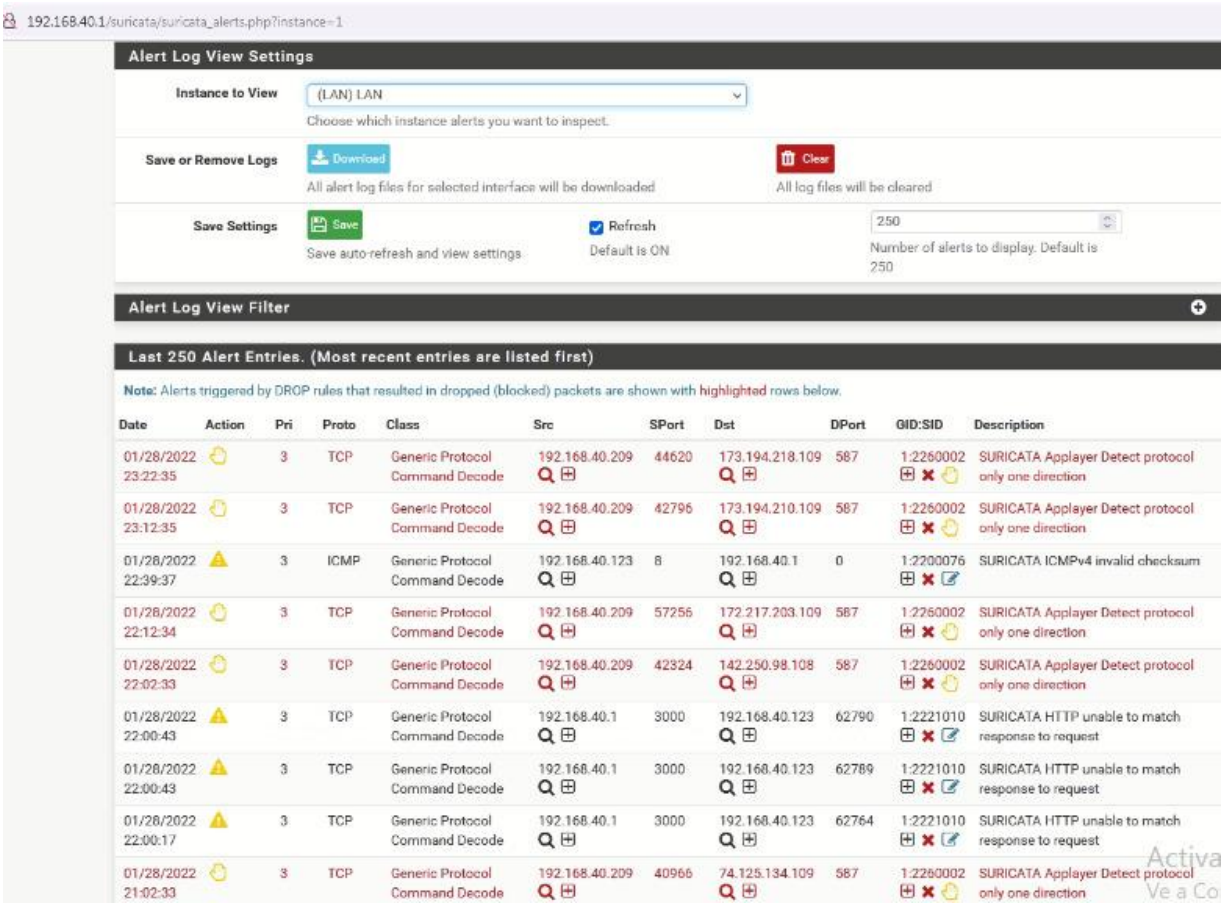


Figura 34. Bloqueo del puerto destino 587
Fuente: Autores

Se define el bloqueo del puerto destino 587 con una prioridad media y la IP origen 192.168.40.209 en la red LAN.

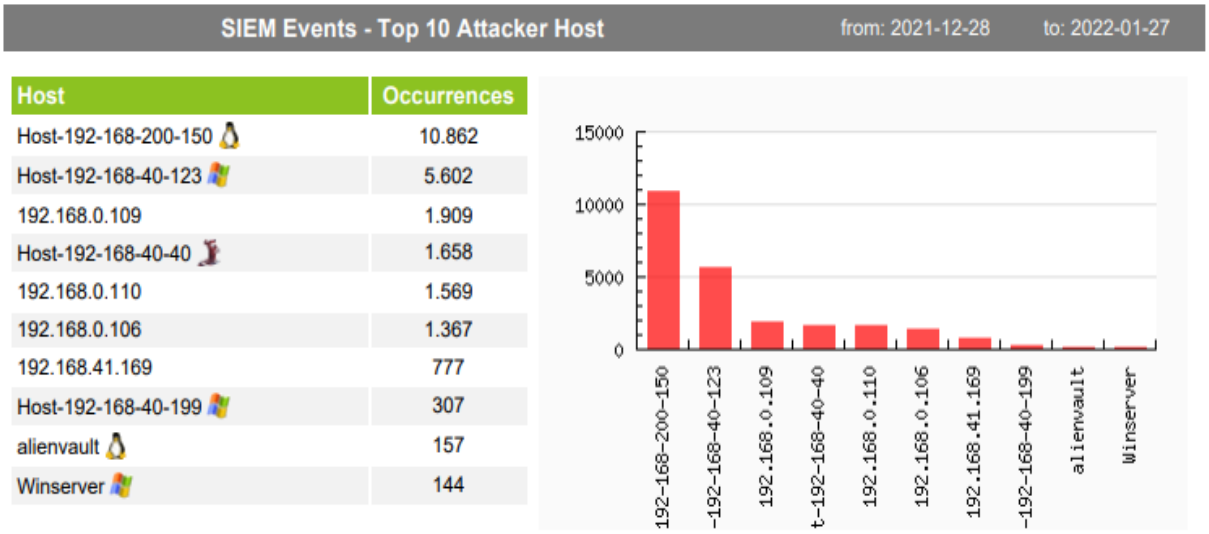


Figura 35. Estadísticas de host Atacantes
Fuente: Autores

Entre los datos de los hosts atacantes que nos presenta la herramienta SIEM en una fecha determinada, en la cual nos muestra los registros de ataques más alto dentro de la red.

Tabla 8. Estadísticas de Host atacantes

HOST	CANTIDAD
192.168.200.150	10.862
192.168.40.123	5.602
192.168.0.109	1.909
192.168.40.40	1.658
192.168.40.199	307

Fuente: Autores

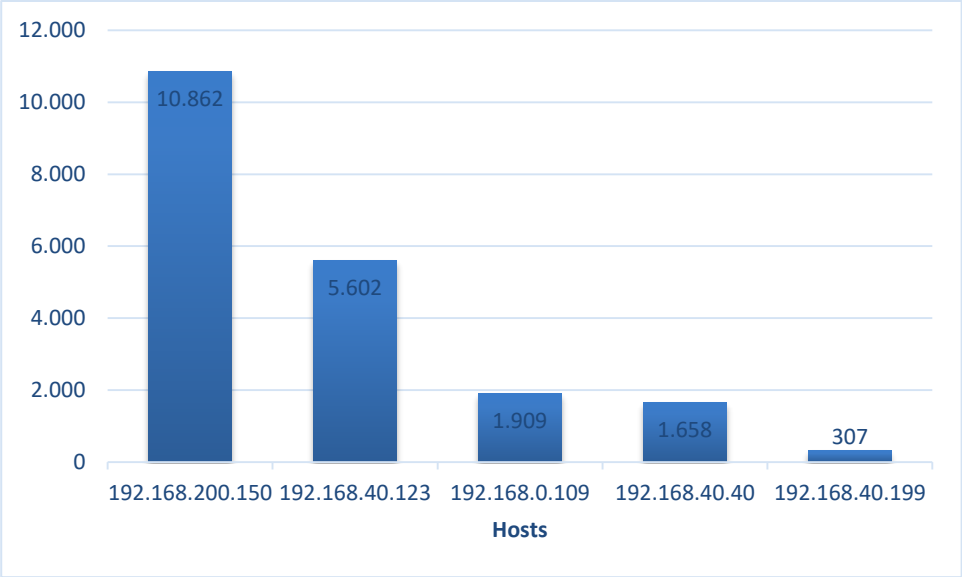


Ilustración 2. Estadísticas de hosts atacantes
Fuente: Autores

En la ilustración 4 se muestra que el equipo que más intentos de ataques dentro de la red LAN del diagrama de red es el equipo Windows con IP 192.168.40.123 con 5602 (cinco mil seiscientos dos) intentos, mientras el dispositivo con el menor número de intentos de ataques es el equipo Ossim AlienVault con IP 192.168.40.199 con 307 (trescientos siete) intentos.

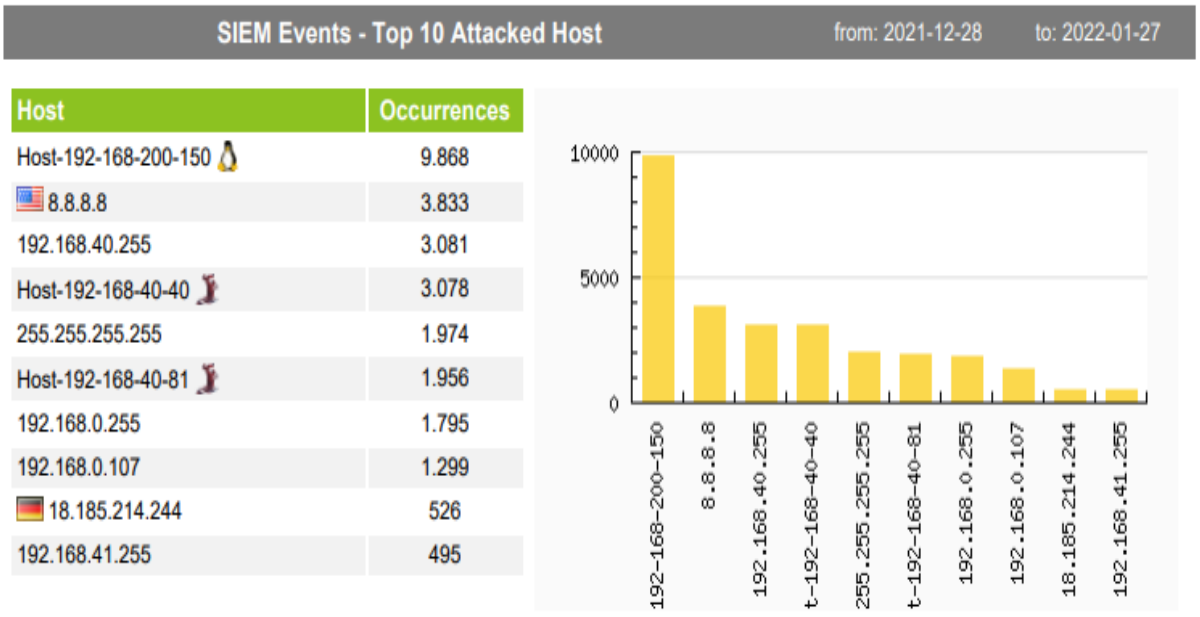


Figura 36. Estadística de Host Atacados
Fuente: Autores

Entre los datos de los hosts atacados que nos presenta la herramienta SIEM en una fecha determinada, nos muestra los hosts con los registros de ataques más altos dentro de la red, entre ellos se encuentra las herramientas FreeNas y Monowall.

Tabla 9. Estadística de Host Atacados

HOST	CANTIDAD
192.168.200.150	9.868
8.8.8.8	3.833
192.168.40.255	3.081
192.168.40.40	3.078
192.168.40.81	1.956
192.168.40.255	495

Fuente: Autores

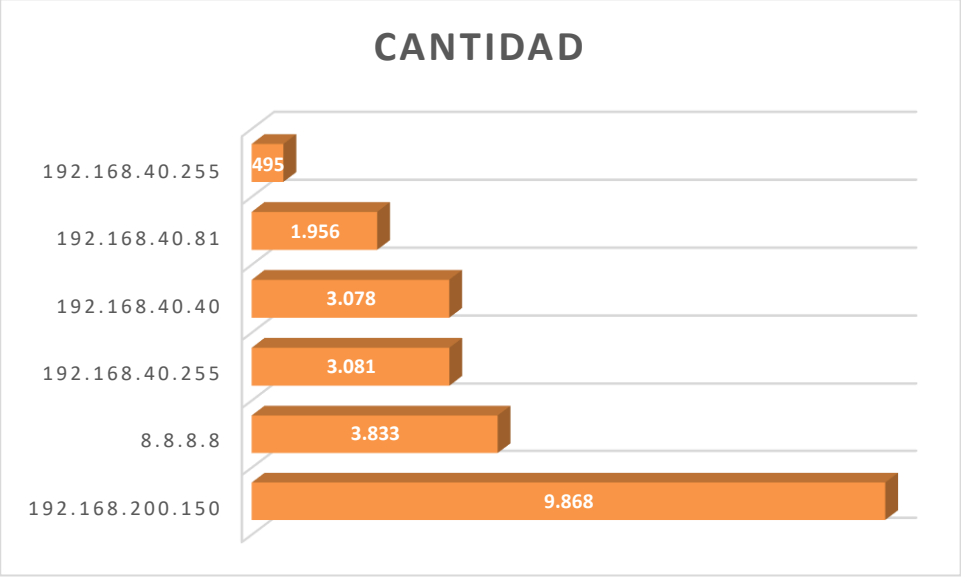
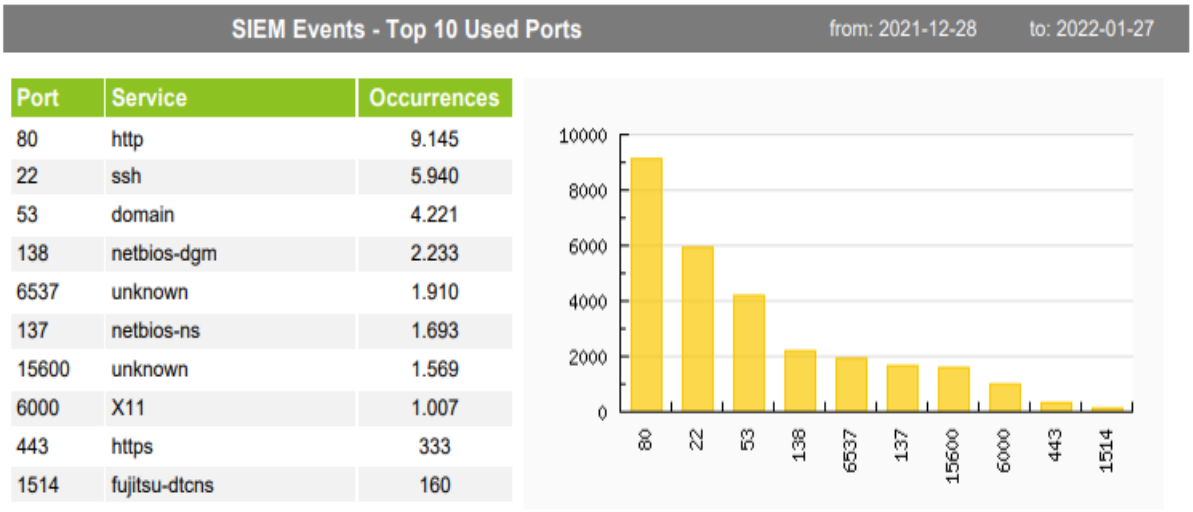


Ilustración 3. Estadística de Host Atacados
Fuente: Autores

Los resultados de los hosts atacados en nuestra red en una fecha determinada, la herramienta SIEM, muestra los hosts con los registros de ataques más altos dentro del diagrama de red, entre ellos mencionamos la herramienta con mayor número de ataques a FreeNas con la IP 192.168.40.40 con un promedio de 3078 (tres mil setenta y ocho) y con menos número de ataques a Monowall con IP 192.168.40.41 con un promedio de 1956 (mil novecientos cincuenta y seis).



SIEM Events - Top 10 Used Ports — from: 2021-12-28 to: 2022-01-27

Port	Service	Occurrences
80	http	9.145
22	ssh	5.940
53	domain	4.221
138	netbios-dgm	2.233
6537	unknown	1.910
137	netbios-ns	1.693
15600	unknown	1.569
6000	X11	1.007
443	https	333
1514	fujitsu-dtcns	160

Figura 37. Estadística de puertos usados
Fuente: Autores

De la misma manera la figura 37, muestra el top de aplicación de puertos más usados en el tráfico de red, siendo el HTTP puerto 80, SSH puerto 22 y puerto DNS 53, los más aplicados de acuerdo con los datos que refleja la herramienta dentro de un rango de fecha.

Tabla 10. Estadística de puertos usados

PUERTO	SERVICIO	CANTIDAD
80	HTTP	9.145
22	SSH	5.940
53	DOMAIN	4.221

138		3.078
6537	UNKNOW	1.910
137	NETBIOS	1.693
443	HTTPS	333

Fuente: Autores

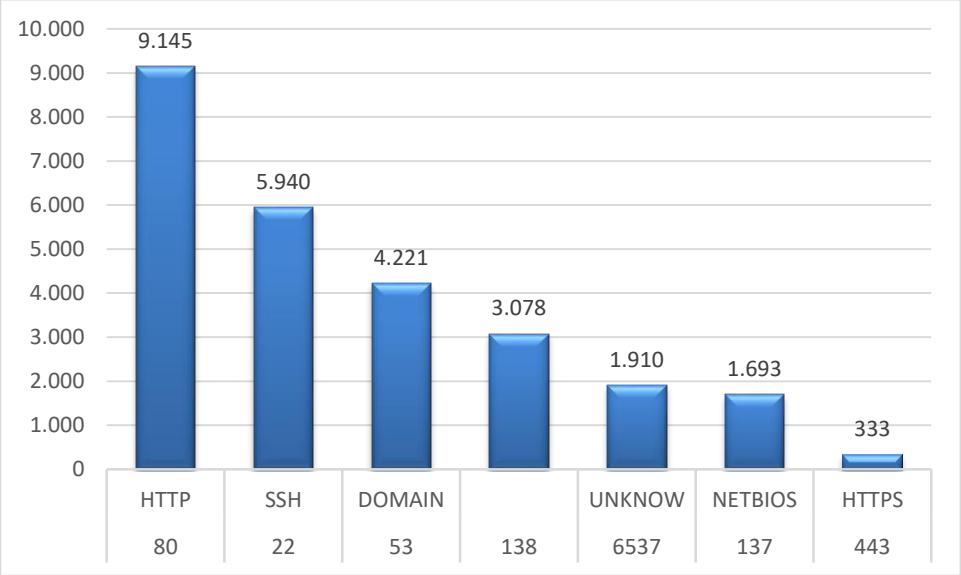
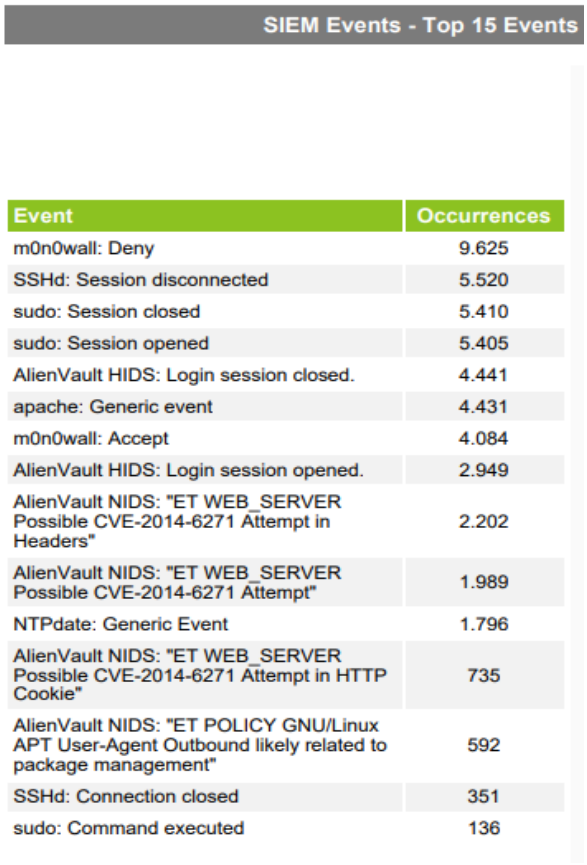


Ilustración 4. Estadística de puertos usados
Fuente: Autores

En la ilustración 6, se describe la detección en un rango de fecha sobre la utilización de los puertos de red, se observa que el puerto más utilizado en la presente topología es el puerto http (80), con un nivel de utilización cercano a 9145(nueve mil ciento cuarenta y uno), y el de menor utilización el puerto https (443), con un nivel de utilización de 333 (trescientos treinta y tres).



SIEM Events - Top 15 Events

Event	Occurrences
m0n0wall: Deny	9.625
SSHd: Session disconnected	5.520
sudo: Session closed	5.410
sudo: Session opened	5.405
AlienVault HIDS: Login session closed.	4.441
apache: Generic event	4.431
m0n0wall: Accept	4.084
AlienVault HIDS: Login session opened.	2.949
AlienVault NIDS: "ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers"	2.202
AlienVault NIDS: "ET WEB_SERVER Possible CVE-2014-6271 Attempt"	1.989
NTPdate: Generic Event	1.796
AlienVault NIDS: "ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Cookie"	735
AlienVault NIDS: "ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management"	592
SSHd: Connection closed	351
sudo: Command executed	136

Figura 38. Estadística de top eventos
Fuente: Autores

A continuación, la herramienta Siem nos muestra un top de los eventos más detectados en un rango de fecha determinado, entre los cuales tenemos un acceso al Monowall como principal evento, una sesión por ssh, sesiones abiertas y cerradas por sudo y de más eventos que se pueden visualizar en la imagen anterior.

Tabla 11. Estadística de top eventos

EVENTO	OCURRENCIA %
Monowall- Deny	22
SSHd: session disconnected	12
Sudo: session closed	12
Sudo: session open	12
AlienVault HIDS: session closed	10

Monowall: accept	9
AlienVault HIDS: session open	7
AlienVault NIDS: "ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers"	5
AlienVault NIDS: "ET WEB_SERVER Possible CVE-2014-6271 Attempt"	4
NTPdate: Generic Event	4
AlienVault NIDS: "ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Cookie"	2
AlienVault NIDS: "ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management"	1

Fuente: Autores

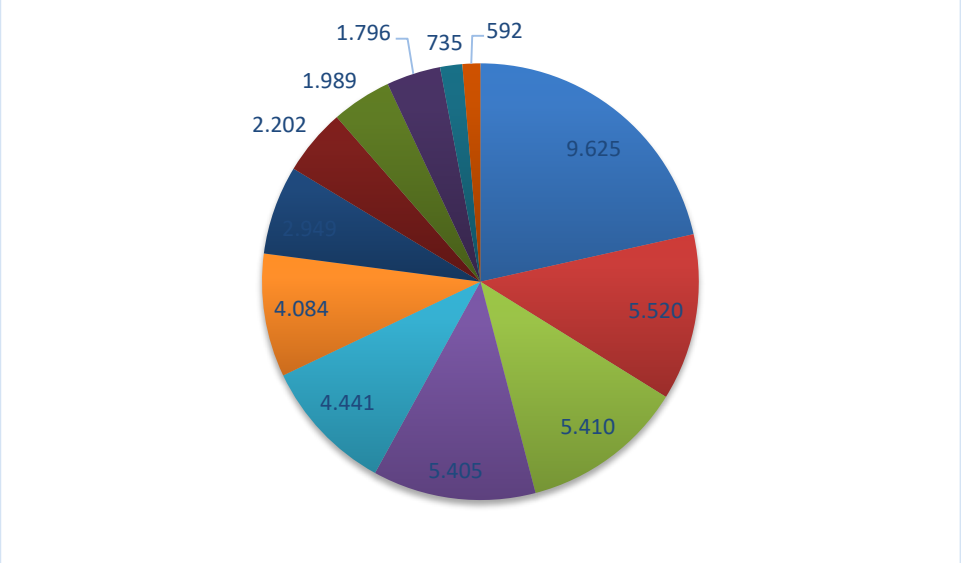


Ilustración 5. Estadística de top eventos
Fuente: Autores

En la ilustración anterior se describe la detección de eventos en un rango de fecha, se observa que el dispositivo de mayor ocurrencia es el Monowall, equivalente al 22% de los eventos colectados, mientras el dispositivo con menor ocurrencia en cuanto a detección de eventos es el dispositivo NTP server correspondiente al 4%.

SIEM Events - Top 15 Events by Risk	from: 2021-12-28	to: 2022-01-27
Event		
AlienVault HIDS: Host-based anomaly detection event (rootcheck).		
AlienVault HIDS: Excessive number of events (above normal)		
AV-FREE-FEED Policy violation, Linux package manager update detected on SRC_IP		
Availability-Monitoring: CURRENT HOST STATE - hard up		
AlienVault HIDS: Physical root login.		
AlienVault HIDS: System user successfully logged to the system.		
SSHd: Session disconnected		
Availability-Monitoring: CURRENT HOST STATE - soft down		
Host operating system change		
Host service change		
sudo: Command executed		
Availability-Monitoring: CURRENT SERVICE STATE - hard ok		
IP address change		
AlienVault NIDS: "ET WEB_SERVER ColdFusion administrator access"		
AlienVault HIDS: Successful sudo to ROOT executed		

Figura 39. Estadística de eventos por riesgo
Fuente: Autores

La imagen muestra el top de los eventos por riesgo en un rango de fecha determinado, entre los cuales tenemos un AlienVault HIDS anomalía, un excesivo número de eventos detectados, ingresos de claves no autorizadas, comandos ejecutados y demás eventos que se pueden visualizar.

Para obtener las estadísticas señaladas anteriormente la herramienta AlienVault Ossim permite generar reportes prediseñados de mucha utilidad, los mismos que pueden ser obtenidos en varios formatos como PDF u hojas de cálculo, para su respectiva revisión y evaluación, se obtienen desde la opción de Reportes del

dashboard de la herramienta AlienVault, en la cual podemos observar que podemos obtener varios reportes con diferentes criterios, formatos y fecha de obtención de los mismos.

4.2. DISCUSIÓN

En el trabajo de Bravo, Villafuerte, & Patiño, (2015), los autores en su análisis señalan que OSSIM, no solo es una herramienta de recolección de logs de diferentes dispositivos, sino un SIEM, que trae incorporado diversas formas de control de seguridad, dando así un aporte invaluable al administrador del centro de datos, dándole información útil para la toma de decisiones ante eventuales anomalías dentro de la red, y al tener la filosofía de código abierto y libre distribución, permite la implementación de una consola centralizada a un costo relativamente bajo.

La "integración de un sistema SIEM como OSSIM el cual permite no sólo la colección de eventos y la monitorización, sino también la detección de diferentes vulnerabilidades y amenazas en tiempo real, así como su análisis y reporte" (Fernández, García, & Garofalo, 2018), así mismo concluyen en su obra proponiendo la instalación de herramientas como "Suricata (con las reglas abiertas de Emerging Threats), ElasticStack para el almacenamiento, análisis y visualización de los registros y eventos de seguridad, e instalar el OpenVAS como escaneador de vulnerabilidades", no obstante dan a conocer que la aplicación de este tipo de sistemas conlleva el uso de recursos a una escala mayor tomando en cuenta si se lo aplicara a una entidad pequeña.

La investigación de Guijarro et al.(2018), indica que la implementación de defensa en profundidad, en sus 7 etapas descritas en su investigación, hace posible mitigar amenazas posibles dentro de una red de forma más eficaz, así mismo el uso de herramientas como Firewall con una red DMZ proporciono robustez a la seguridad perimetral y evito quedar expuestos ante ataques externos,

recomendando ambas investigaciones el uso de herramientas como el sistema detector de intrusos en la Red (NISD) para añadir una capa más de seguridad.

La herramienta SIEM según Quintero & Tovar (2019), no debe ser tomado como simple medio para eliminar problemas o anomalías de seguridad, si no como un disparador para introducir métodos y mecanismos de solución ante los posibles ataques cibernéticos, ya sea por algún proceso automatizado, la intervención de un administrador de los recursos, o incluso la intervención de un equipo de respuestas a incidentes, así como de otros relacionados a la mejora continua y optimización de los recursos tecnológicos.

Según Montesino (2013), en su investigación la gestión de la seguridad informática implica un trabajo complejo para los encargados de la seguridad por el gran número de controles en varios entornos, por ende para aumentar la efectividad y reducir la complejidad y amenazas es posible automatizar determinadas acciones y controles, sin intervención humana en esas acciones, proponiendo en su investigación el uso de los sistemas SIEM, mediante la definición de conectores, políticas, reglas de correlación y reportes de seguridad informática. Dando una propuesta de uso del sistema SIEM de software libre OSSIM. Basado en el resultado de la investigación se concluye que la utilización de este tipo de herramientas aumentan la efectividad de poder mitigar posibles ataques anómalos que puedan desafectar la infraestructura de red y tener un control centralizado y aumentar su potencial de automatización.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- La investigación presenta el estado actual de la infraestructura de red con un diseño basado en las 7 capas del modelo de defensa en profundidad para el HEP, lo que permitió tomar decisiones claras basados en Sistemas de correlación de logs, monitorizando en tiempo real el comportamiento de la red, por medio de controles y reglas que garantiza la seguridad, integridad y la disponibilidad, evitando así anomalías en la red y fallos en sus servicios.
- Dentro de los sistemas de correlación de logs se escogió la utilización de la herramienta AlienVault OSSIM para el análisis de logs, los mismos que son recolectados desde los dispositivos conectados nos permiten descubrir posibles anomalías, todo esto converge en las demás herramientas integradas para el monitoreo y detección dentro del OSSIM entre las que tenemos Firewall, IDS, IPS, WAF, así mismo por estar integradas estas herramientas en una sola plataforma permiten tener una gestión centralizada de la seguridad.
- Para la implementación de un sistema de seguridad centralizada y de Correlación de eventos de log como AlienVault OSSIM brinda información útil al administrador de red permitiendo la toma de decisiones y mejorando la seguridad, se han integrado diferentes dispositivos de red de varias marcas así como diversos servicios en una misma consola de gestión, permitiendo lograr resultados confiables según la implementación realizada. Los costos son relativamente bajos con la herramienta AlienVault OSSIM debido a que es una distribución libre además de tener una consola centralizada.
- Con el despliegue de ataques informáticos en ambiente controlado y en ambiente de producción apoyados en las directrices de OSSTMM, tenemos: puertos escaneados, inyección SQL, Denegación de Servicio DoS, Payloads y Fuerza Bruta, en los cuales se comprobó la veracidad en

el descubrimiento de eventos anómalos en la red gestionados por la herramienta basada en correlación de logs AlienVault OSSIM.

- La elaboración del plan fortalecimiento ante ataques informáticos contempla una guía de la gestión y aplicabilidad de seguridad de defensa en profundidad basada en correlación de eventos de logs para la Unidad de Tecnología de la Información y Comunicación del HEP.

5.2. RECOMENDACIONES

- Se recomienda la utilización de la herramienta AlienVault como un sistema muy poderoso al momento de observar la disponibilidad de los equipos de red, proporcionando una gran fiabilidad en los momentos donde se presenten anomalías en la infraestructura tecnológica, así mismo presenta un gran volumen de información el cual se puede analizar a muy detalle.
- Se exhorta al administrador de TI profundizar sus conocimientos en el área de ciberseguridad y administración de sistemas Unix y así explotar al máximo las bondades proporcionada por la herramienta AlienVault.
- Es recomendable por cuestiones de seguridad configurar una de las interfaces de red de la herramienta SIEM únicamente para su administración, de igual manera contar con un servidor ntp con la hora actualizada en la que todos los dispositivos que intervienen en la infraestructura se sincronicen.
- Utilizar la estrategia de defensa en profundidad garantizara que se mantenga un perfil de seguridad de la información adecuada y eficaz. La idea es colocar al menos un control en cada línea de defensa y hacer uso de soluciones de automatización para tener la capacidad de autocorregirse y notificar de inmediato el evento generado, mantener visualizado nuestro entorno es el secreto.
- Se recomienda la ejecución del plan de fortalecimiento ante ataques informáticos basado en correlación de log.

BIBLIOGRAFÍA

Agrawal, K., & Makwana, H. (2013). Un estudio sobre capacidades críticas para la seguridad de la información y la gestión de eventos. En Revista Internacional de Ciencia e Investigación (Vol. 4). www.ijsr.net

Alvino, C. (2021, May 5). Estadísticas de la situación digital de Ecuador en el 2020-2021 | Branch. https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-ecuador-en-el-2020-2021/

Ambit. (2019, May 20). La estrategia de seguridad en las bases de datos. https://www.ambit-bst.com/blog/la-estrategia-de-seguridad-en-las-bases-de-datos

Ariu, D., Frumento, E., & Fumera, G. (2017). Ingeniería social 2.0: un trabajo fundamental: artículo invitado. erudito semántico, 319–325. https://doi.org/10.1145/3075564.3076260

Avast. (2021, May 19). ¿Qué es un Cross-Site Scripting (XSS)? | Cómo sucede | Avast., de Avast Academy website: https://www.avast.com/es-es/c-xss

Bowling, J. (2010). *AlienVault: el futuro de la gestión de la información de seguridad* | *Diario Linux.* https://www.linuxjournal.com/article/10649?page=0%2C0

Bravo, H., Villafuerte, L., & Patiño, J. (2015). *Implantación De Una Herramienta Ossim Para El Monitoreo Y Gestión De La Seguridad De La Red Y Plataformas Windows Y Linux Aplicado A Empresas Medianas*. http://www.dspace.espol.edu.ec/handle/123456789/29939

CEH. (2020). Hacker ético certificado | Certificación CEH | CEH v11 | Consejo CE., https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

Cordova, J., Vega, H., Rodriguez, C., & Escobedo, F. (2020). FIRMA DIGITAL BASADA EN CRIPTOGRAFÍA ASIMÉTRICA PARA GENERACIÓN DE HISTORIAL CLÍNICO. *3c Tecnologias*, *9*(2254 – 4143), 65–85. https://scholar.google.com/citations?view_op=view_citation&hl=es&user=VhTwpWwAAAAJ&citation_for_view=VhTwpWwAAAAJ:qjMakFHDy7sC

Cornaglia, S., & Vercelli, A. H. (2017). La ciberdefensa y su regulación legal en Argentina (2006-2015)/ La ciberdefensa y su regulación jurídica in Argentina (2006-2015). *URVIO - Revista Latinoamericana de Estudios de Seguridad*, (20), 49–62. https://doi.org/10.17141/urvio.20.2017.2601

Davyt, M. (2017). SIEM: Hacia una nueva estrategia de ciberseguridad. *Revista de Negocios Del IEEM*, 64–65. https://www.haceremprendimiento.pdf

Fernández, A., García, L., & Garofalo, A. (2018). Propuesta de controles de seguridad

para nubes privadas y centros de datos virtualizados. *Telemática*, *17*(1), 56–72. https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/290

Fidias, A. (2017). *EL PROYECTO DE INVESTIGACION FIDIAS ARIAS 7MA EDIC 2016.pdf - Free Download PDF* (7th ed.). Caracas: Episteme. https://kupdf.net/download/el-proyecto-de-investigacion-fidias-arias-7ma-edic-2016pdf_5a1b4afde2b6f5e526da642c_pdf

Guijarro, A., Yepez, J., Peralta, T., & Ortiz, M. (2018). No Titulo. *Revista Espacios*, *39*(0798 1015), 19–27.

Hernández, A., & Mejía, J. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *Revista Electronica de Computacion, Informatica Biomedica y Electronica*, 1–18.

Hernández, M. (2019, September 2). En América Latina se registran 45 ataques cibernéticos por segundo • Tecnología • Forbes México. https://www.forbes.com.mx/en-america-latina-se-registran-45-ataques-ciberneticos-por-segundo/

Herzog, P. (2010). *OSSTMM*. ISECOM. www.osstmm.org

INCIBE. (2015, May 21). DoS: Capa de Aplicación | INCIBE-CERT. https://www.incibe-cert.es/blog/dos-capa-aplicacion

Insurance Journal. (2016, May 24). Los ladrones de ciberbancos robaron $ 12 millones del banco de Ecuador en 2015, utilizando el sistema SWIFT. https://www.insurancejournal.com/news/international/2016/05/24/409577.htm

IONOS. (2020, October 1). SYN flood: métodos de ataque y medidas de protección - IONOS. https://www.ionos.es/digitalguide/servidores/seguridad/syn-flood/

Jhony, E., & Alvarado, Y. (2015). LOS DELITOS INFORMÁTICOS Y SU PENALIZACIÓN EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL ECUATORIANO. *Universidad Politécnica Estatal Del Carchi*, *8*, 171–194.

Juan, M., Luis, M., Carlos, M., & Juan, O. (2008). (PDF) Implementación y mejora de la consola de seguridad informática OSSIM una experiencia de colaboración universidad-empresa. *ResearchGate*, *6*, 29–37. https://www.researchgate.net/publication/279490894_Implementacion_y_mejora_de_la_consola_de_seguridad_informatica_OSSIM_una_experiencia_de_colaboracion_universidad-empresa

Kavanagh, K. M., & Rochford, O. (2015). *Cuadrante Mágico de Información de Seguridad y Gestión de Eventos Cuadrante Mágico de Información de Seguridad y Gestión de Eventos Cuadrante Mágico Figura 1. Cuadrante Mágico de Información de Seguridad y Gestión de Eventos CRITERIOS DE EVALUACIÓN DEFINICIONES.* http://www.gartner.com/technology/reprints.do?id=1-2JNR3RU&ct=150720&st=sb

La Republica. (2021, March 24). *Aumenta la preocupación por la ciberseguridad en Latinoamérica | La República EC*.

https://www.larepublica.ec/blog/2021/03/24/aumenta-la-preocupacion-por-la-ciberseguridad-en-latinoamerica/

Miller, D., Harris, S., Harper, A., Vandyke, S., & Black, C. (2010). Implementación de Gestión de Eventos e Información de Seguridad (SIEM). McGraw-Hill Osborne Media. https://mhebooklibrary.com/doi/book/10.1036/9780071701082

Montesino, R., Garcia, W., & Porven, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *Revista Ingeniería Electrónica, Automática y Comunicaciones*, *34*(1), 40–58. https://doi.org/10.1234/RIELAC.V34I1.152

Müller, A. (2009). *Motor de correlación de eventos.* 31–57.

NTOP. (n.d.). ntop – Soluciones de monitoreo de red de alto rendimiento basadas en código abierto y hardware básico. https://www.ntop.org/

OpenVas. (n.d.). OpenVAS - Abra el Escáner de evaluación de vulnerabilidades. de https://www.openvas.org/

OSI. (2018, August 21). ¿Qué son los ataques DoS y DDoS? | Oficina de Seguridad del Internauta. https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

Quintero, M., & Tovar, S. (2019). Sistema de Gestion de Informacion y Eventos de Seguridad (SIEM. *Tecnologias de Informacion En Eduacacion Superior TIES*, *1*, 30–36. https://www.ties.unam.mx/num02/pdf/num02.pdf

Raudales, C. (2017). La Brecha Existente En La Ciberseguridad En Honduras. *Innovare Ciencia y Tecnología*, 58–73.

Rodriguez, L. (2016). Integración de un sistema de detección de intrusos y un escáner de vulnerabilidades para la detección efectiva de ataques informáticos. *Universidad de Las Ciencias Informáticas*, *9*, 51–69.

Snort. (n.d.). Guías de configuración de Snort para la prevención de amenazas emergentes. https://www.snort.org/documents

Tom Bergin, & Nathan Layne. (2016). *Informe especial: Los ladrones cibernéticos explotan la fe de los bancos en la red de transferencia SWIFT | Reuters. Londres/Chicago.* https://www.reuters.com/article/us-cyber-heist-swift-specialreport/special-report-cyber-thieves-exploit-banks-faith-in-swift-transfer-network-idUSKCN0YB0DD

ANEXOS

ANEXO 1. FASE DE IMPLEMENTACION

Instalación y configuración de máquinas virtuales y físicas presentes en la infraestructura de red propuesta

- **VMWare Workstation 16**

Se procede con la instalación de la herramienta VMWare Workstation como se observa en las siguientes imágenes, figura 40

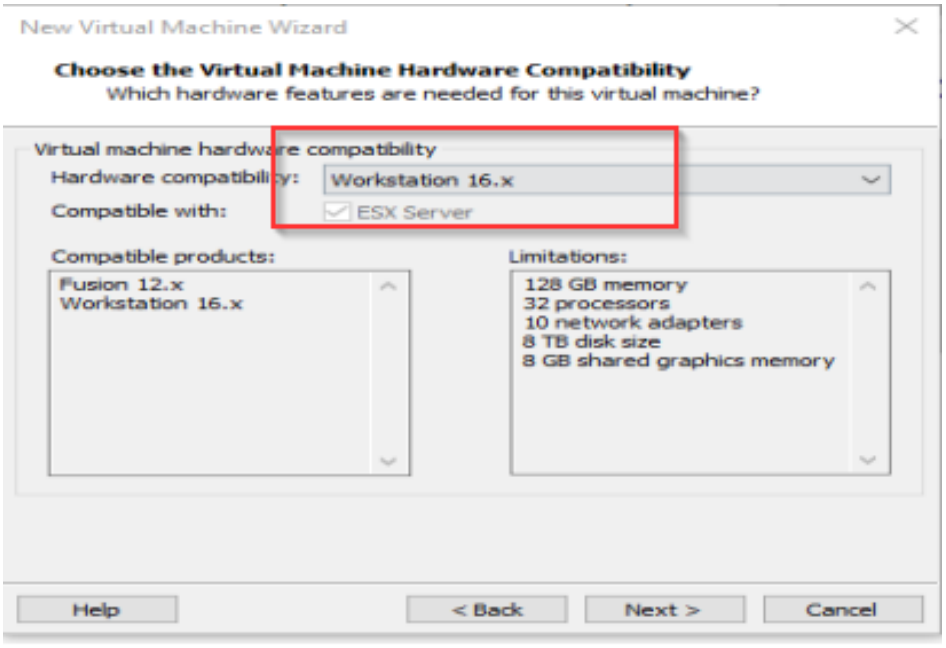


Figura 40. Instalación de Sistema Paravirtualización
Fuente: Autores

Una vez culminada la instalación de la herramienta de virtualización podemos observar la siguiente interfaz, a partir de este punto se procede con la creación de las máquinas virtuales y posteriormente la instalación del sistema operativo y configuraciones iniciales en cada uno de los dispositivos que intervienen en el diagrama de red propuesto.

- **FREENAS**

Una vez realizada la creación de la máquina virtual en el sistema de virtualización se procede con la instalación y configuración de la herramienta, en este caso se instalará y configurará la herramienta FREENAS, la misma que servirá como un sistema de almacenamiento en red, esta NAS está en el Sistema Operativo Free-BSD, para la instalación de la presente máquina virtual seguimos los siguientes pasos, en la figura 18 se muestra el resumen de la configuración de la máquina virtual FreeNas.

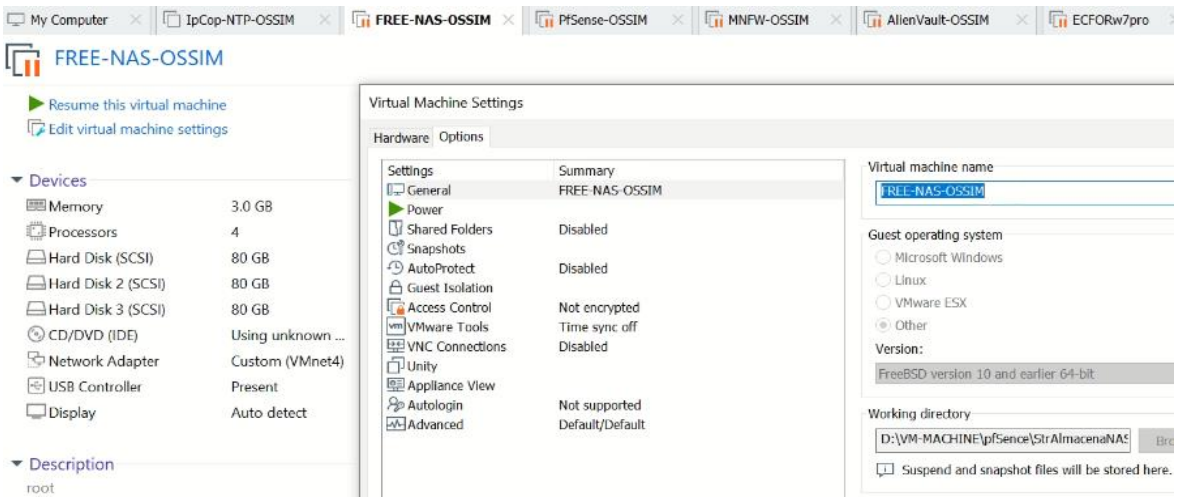


Figura 41. Instalación de FreeNas
Fuente: Autores

Al arrancar la imagen iso y escoger la opción de instalación del sistema operativo FreeNAS, nos solicita la asignación de la interfaz de red, para ello se selecciona el número del menú como se muestra en la figura 41.

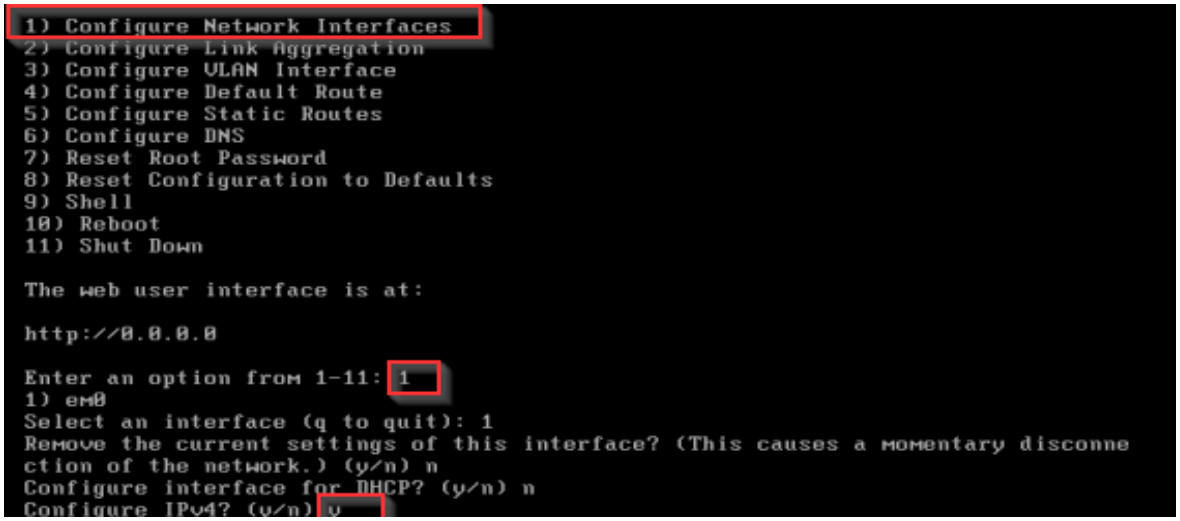


Figura 42. Instalación de FreeNas
Fuente: Autores

Una vez asignada la interfaz y configurada la dirección de red asignada, se procede a reiniciar el sistema operativo para que los cambios surjan efecto y la máquina virtual pueda ser administrada mediante la consola de gestión web como se observa en la figura 45.

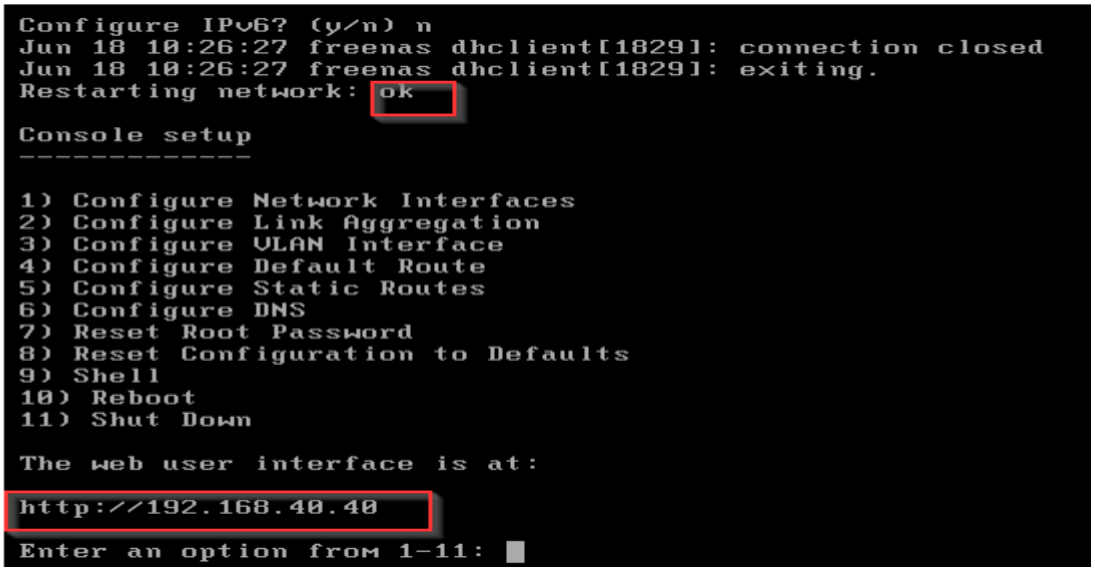


Figura 43. Configuración FreeNas
Fuente: Autores

La administración o gestión de las máquinas virtuales las realizaremos mediante el la interfaz de la máquina virtual Windows 7, la misma que estará interconectada a través de la red LAN del laboratorio propuesto, como se observa en la figura 43, el cual nos muestra la interfaz de gestión web de la máquina virtual FREENAS.

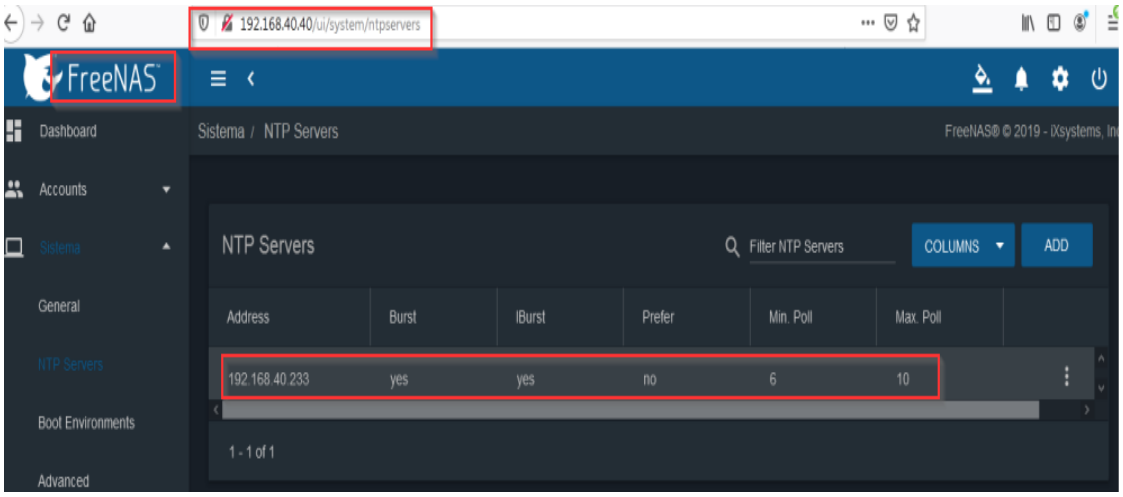


Figura 44. Panel de Control de FreeNas
Fuente: Autores

Así mismo observamos que este y todas las máquinas virtuales o dispositivos que intervienen en la presente topología de red estarán interconectados y sincronizados a la misma hora, por tal motivo estarán sincronizados con el NTP el cual está corriendo en la máquina virtual IPCOP.

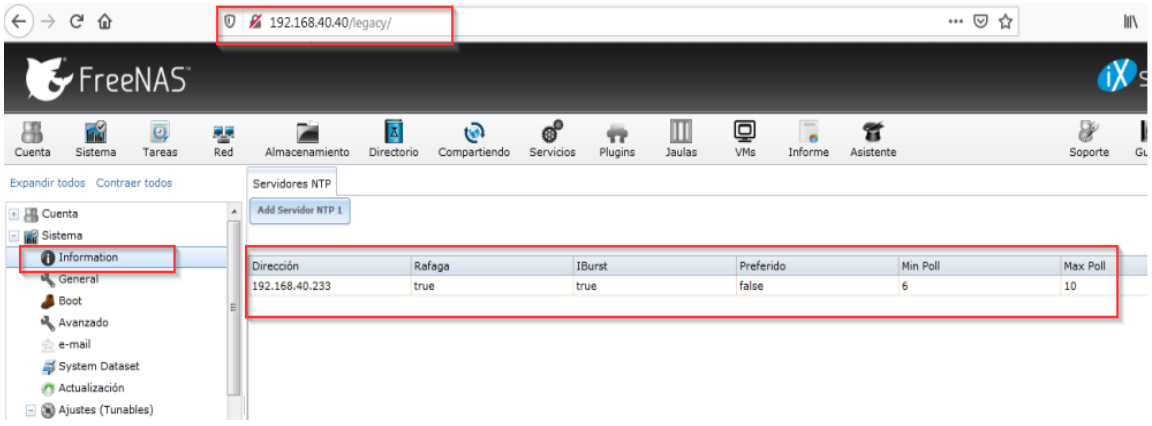


Figura 45. Información FreeNas
Fuente: Autores

- **PFSENSE**

Una vez configurada la máquina virtual en el sistema de virtualización presentamos el resumen de la configuración para la presente herramienta, la cual podemos observar en la figura 46 cabe mencionar que la presente VM está configurada con 2 interfaces de red para los fines que se utilizará en la presente investigación.

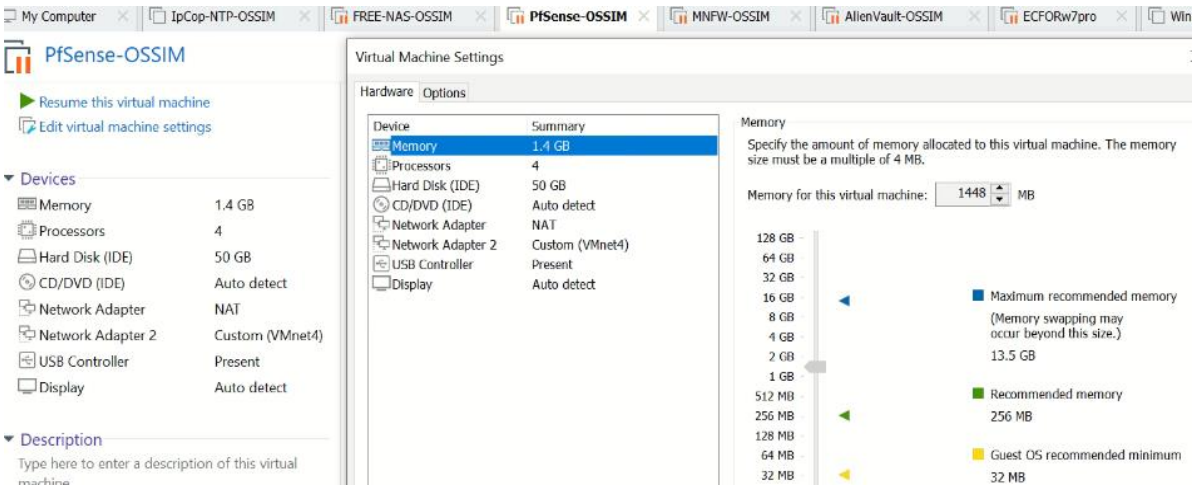


Figura 46. Configuración VM PFSENSE
Fuente: Autores

Al arrancar la imagen iso del sistema operativo Pfsense observamos una pantalla de bienvenida en la cual debemos escoger la opción para proceder con la instalación como se observa en la figura 47.

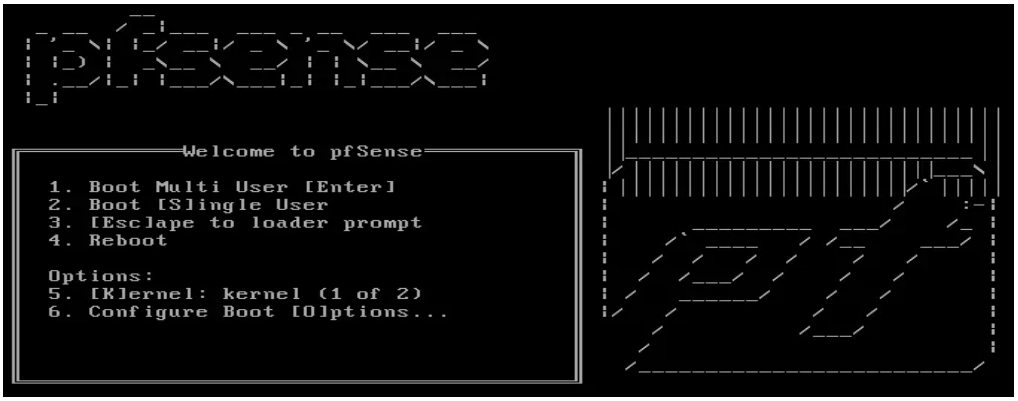


Figura 47. Instalación PFSENSE
Fuente: Autores

Una vez que damos ENTER para empezar con la instalación nos solicita aceptar el acuerdo de licenciamiento de Pfsense, posterior a ello procedemos a seleccionar la opción de instalar como se muestra en figura 48.

Figura 48. Instalación PFSENSE
Fuente: Autores

Una vez realizada la instalación nos solicita que debemos reiniciar el sistema operativo para finalizar la instalación, posteriormente procedemos a configurar las interfaces de red, para ello escogemos la opción del menú 2 que nos permite configurar IP estáticas para nuestro caso como observamos en la figura 49.

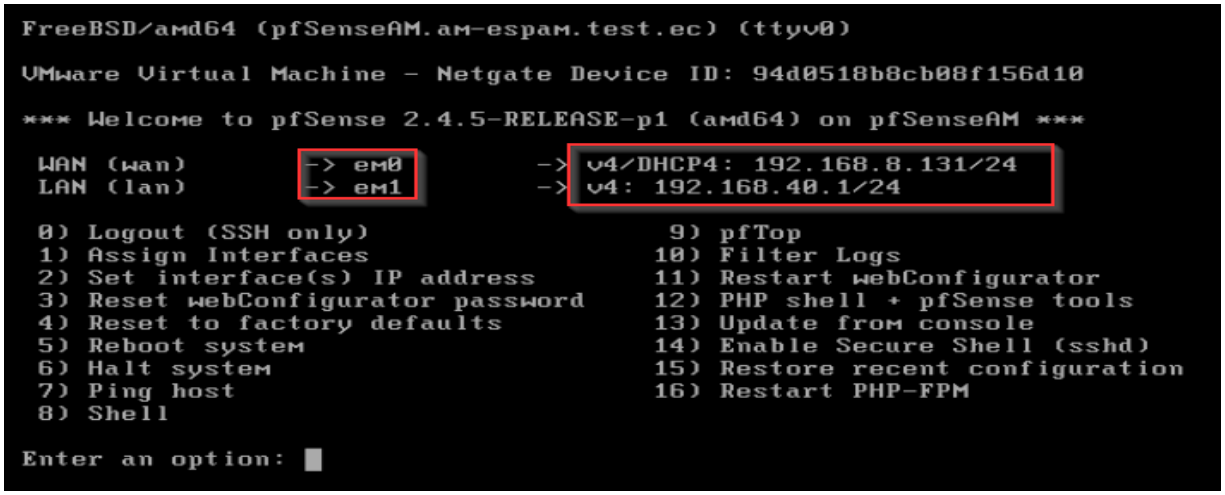


Figura 49. Configuración interfaces PFSENSE
Fuente: Autores

Observamos que se configuran las 2 interfaces LAN y WAN como se encuentra definido en nuestro esquema de red, permitirá la funcionalidad de acceso mediante VPN a nuestra red LAN.

Así mismo podemos observar en la figura 50 la administración o gestión de esta herramienta mediante su acceso web, el mismo que realizamos a través de la pc con Windows 7.

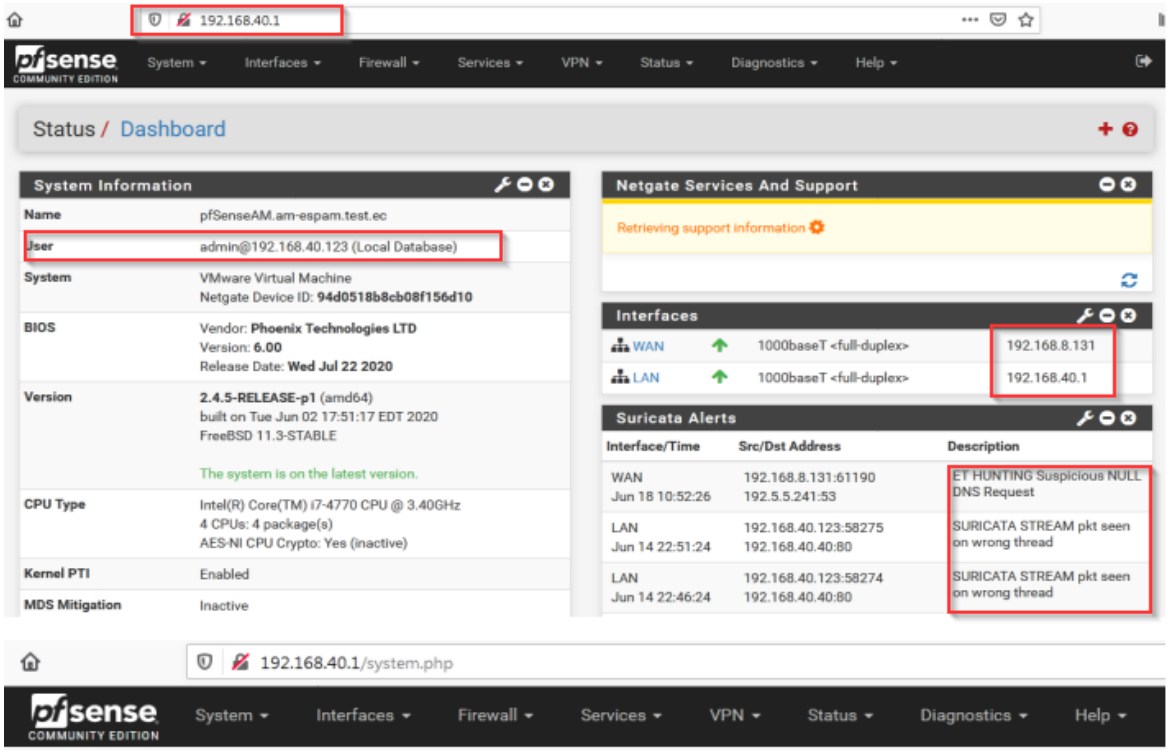


Figura 50. Gestión Web PFSENSE
Fuente: Autores

Como todas las maquinas o dispositivos de red que intervienen en el presente laboratorio, se procede con la configuración del NTP como se observa en la figura 51.

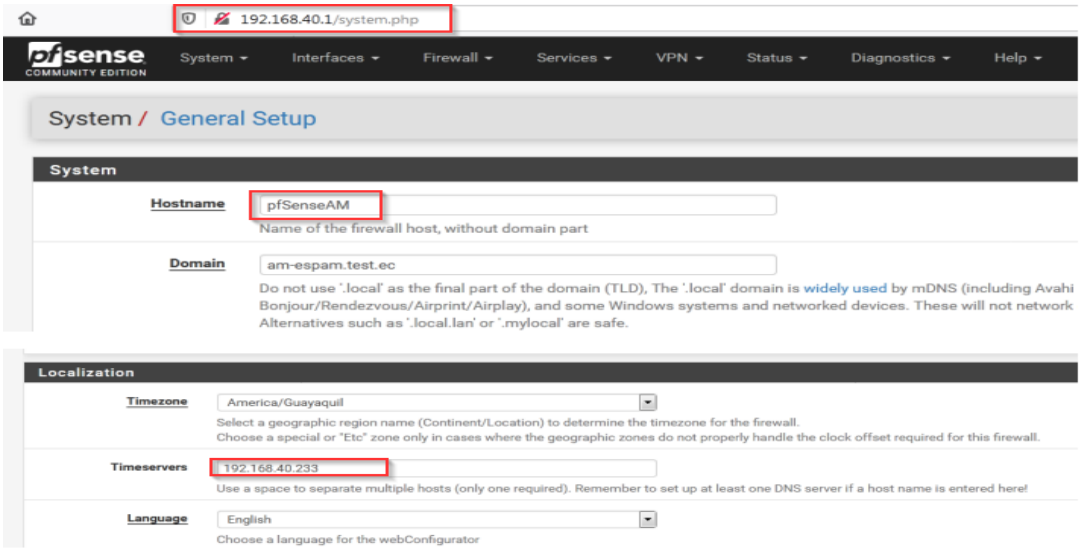


Figura 51. Configuración NTP en PFSENSE
Fuente: Autores

Continuando con la configuración del FW PfSense procedemos a instalar y configurar varios de los paquetes necesarios o herramientas a utilizar en nuestra implementación virtual, como ya nombramos anteriormente, entre los cuales podemos citar NET-SNMP, NTOPNG, SURICATA, entre otros como se visualiza en la figura 52.

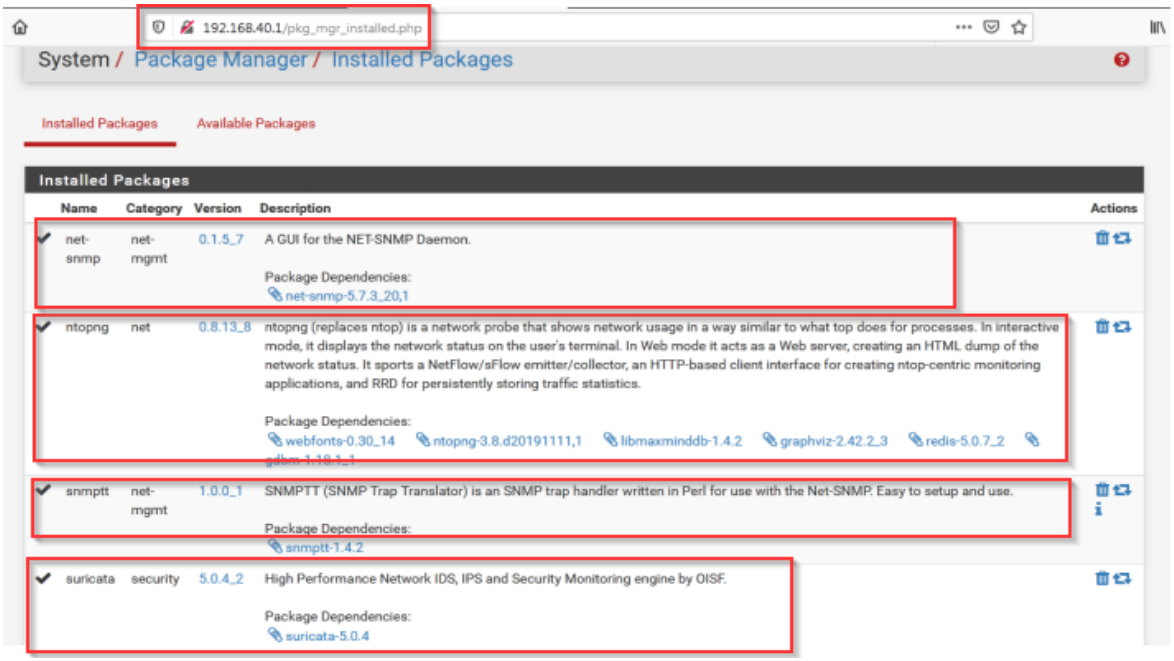


Figura 52. Instalación de Paquetes
Fuente: Autores

El tipo de implementación propuesta como se mencionó anteriormente es mediante una seguridad centralizada, en la cual intervienen como ente correlacionador la herramienta OSSIM, la misma cuenta con detectores que permitirán escuchar y poder aprender de los eventos que ocurren en la red, para esto se debe configurar en cada máquina virtual o dispositivos que interviene en la red hacia donde se van a enviar dichos datos, para ello configuramos la interfaz de escucha del dispositivo que almacenara esta data, el cual estaremos hablando más adelante, se deja estipulada la configuración en el presente FW Pfsense en la figura 53.

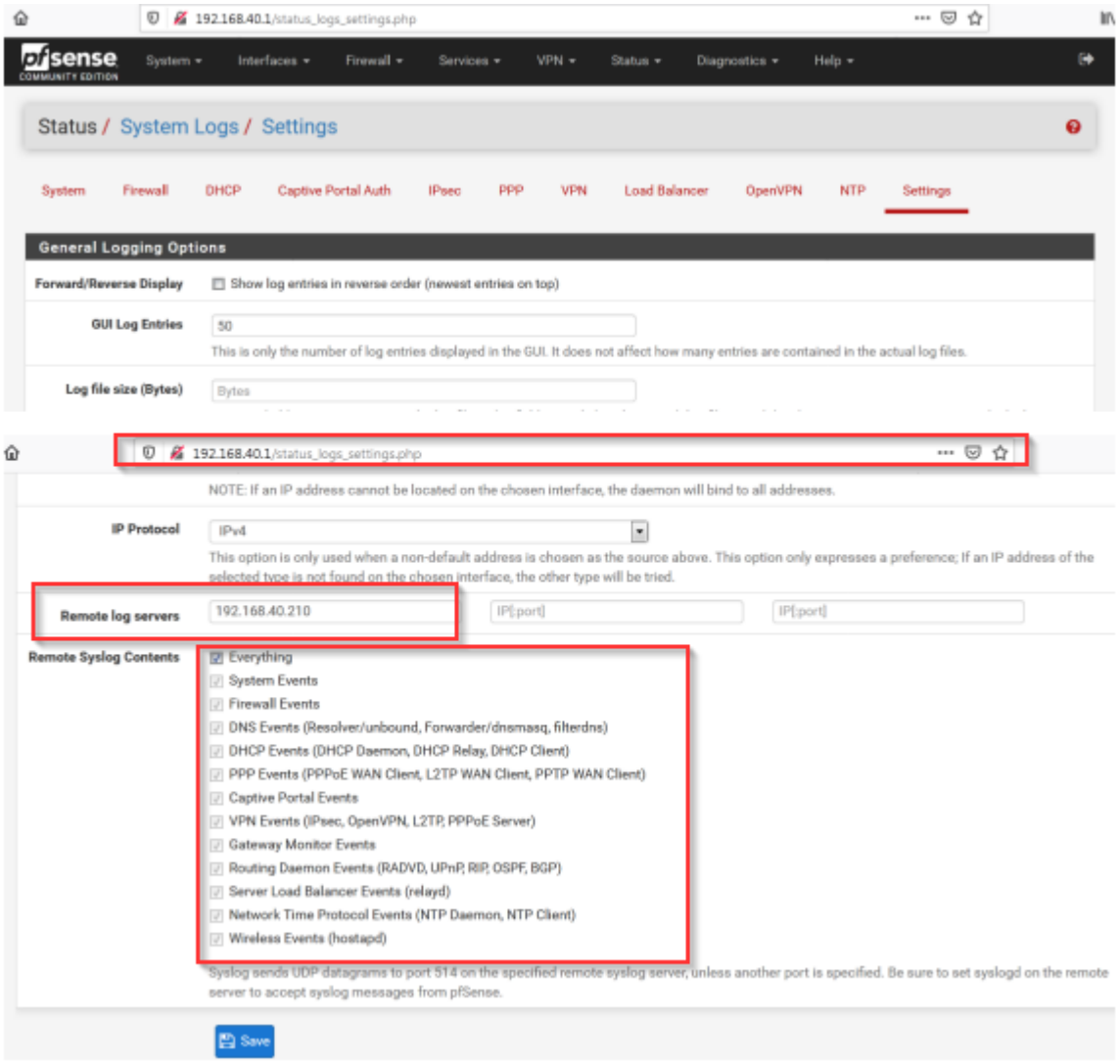


Figura 53. Configuración envío de logs a server remoto
Fuente: Autores

- **IPCOP**

Continuando con la instalación y configuración de los diferentes componentes que intervienen en la presente propuesta de investigación, procedemos a configurar la máquina virtual para el FW IPCOP, mostramos un resumen de la configuración de la VM en la figura 54.

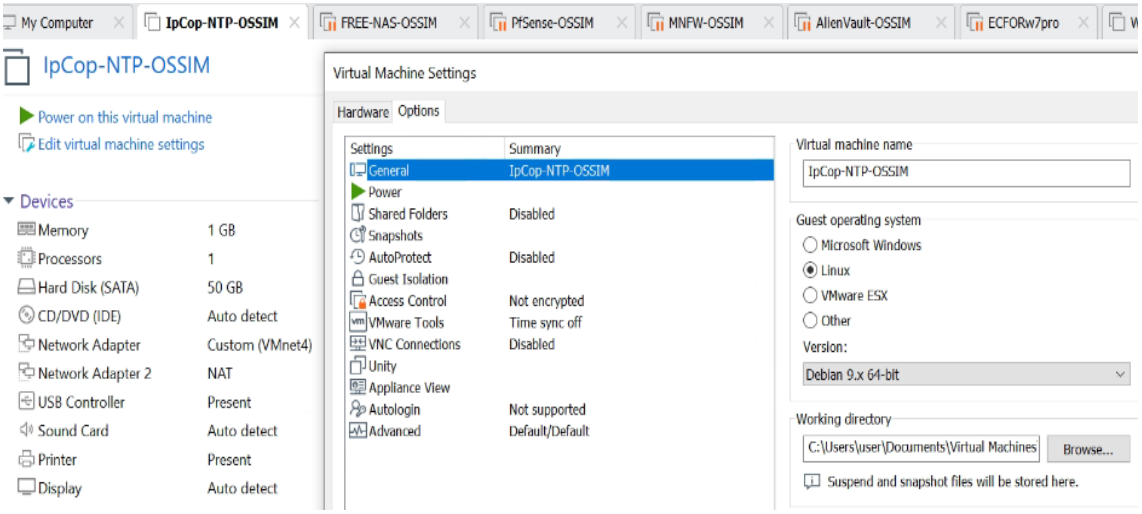


Figura 54. Configuración VM IPCOP
Fuente: Autores

La herramienta IPCop es una herramienta basada en Linux tipo appliance, el rol que desempeñará en la presente investigación es puramente de NTP (Network Time Protocol), pone el horario en la red, aunque también se puede utilizar en muchas otras funcionalidades como intrusión proxy, proxy cache, vpn, entre otros, observamos la figura 55 que nos muestra la pantalla inicial para comenzar con la instalación de esta herramienta.

Figura 55. Instalación IPCOP
Fuente: Autores

Una vez que damos a enter para comenzar con la instalación del sistema operativo procedemos a seleccionar el origen de la instalación por lo general cd-rom o .iso en su defecto para VM, así mismo seleccionamos la configuración automática de la unidad de disco, después de aquello procedemos a probar para que nos detecte las interfaces de red como se observa en la figura 56.

Figura 56. Prueba interfaces IPCOP
Fuente: Autores

Posterior a aquello entramos a la configuración de red de cada una de las interfaces para la presente investigación contamos con 2 interfaces nombradas por el SO como green y red respectivamente como se observa en la figura 57.

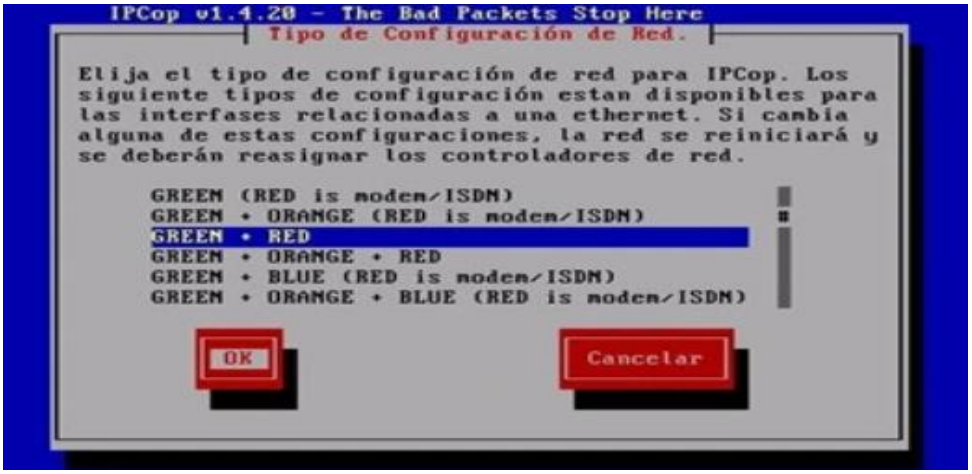


Figura 57. Configuración interfaces IPCOP
Fuente: Autores

De manera similar como con los otros dispositivos que intervienen en el diagrama de red propuesto podemos gestionar dicho sistema operativo de manera remota mediante un gestor web como se observa en la figura 58, en el mismo podemos observar la configuración del IPCOP como un servidor netamente NTP, el cual se ha visto reflejado en las configuraciones de equipos anteriores, esto por la importancia de manejar datos síncronos.

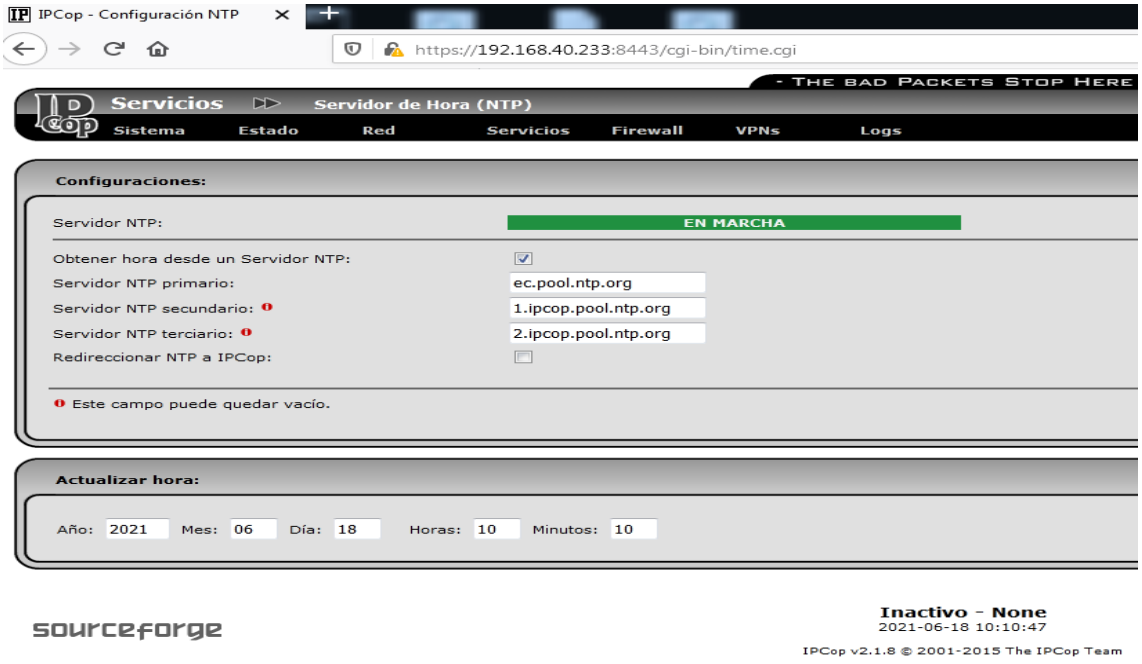


Figura 58. Configuración interfaces IPCOP
Fuente: Autores

Figura 59 IPCop – Ntop configuración
Fuente: Autores

- **MONOWALL**

Continuando con la instalación y configuración de los diferentes componentes que intervienen en la presente propuesta de investigación, procedemos a configurar la máquina virtual para el FW MONOWALL, mostramos un resumen de la configuración de la VM en la figura 60.

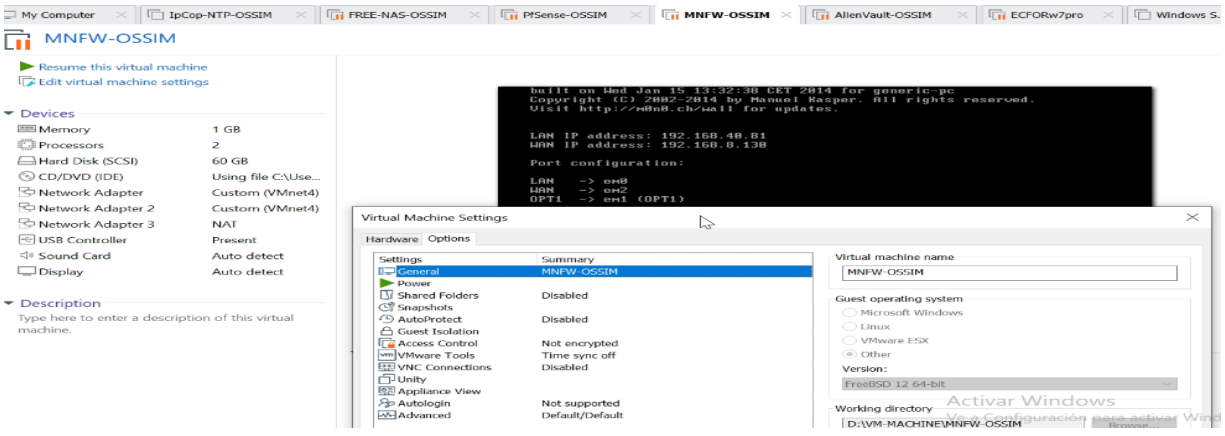


Figura 60. Configuración VM MONOWALL
Fuente: Autores

La herramienta Monowall es una herramienta firewall basada en sistema operativo Free-BDS tipo appliance de libre distribución, el rol que desempeñará en

la presente investigación es de firewall y syslog, aunque también se puede utilizar en muchas otras funcionalidades, está configurado para ser utilizado con 3 interfaces de red que representan o se asignan a la DMZ (zona desmilitarizada) zona LAN y zona WAN, observamos la figura 64 que nos muestra la pantalla inicial para comenzar con la instalación de esta herramienta.

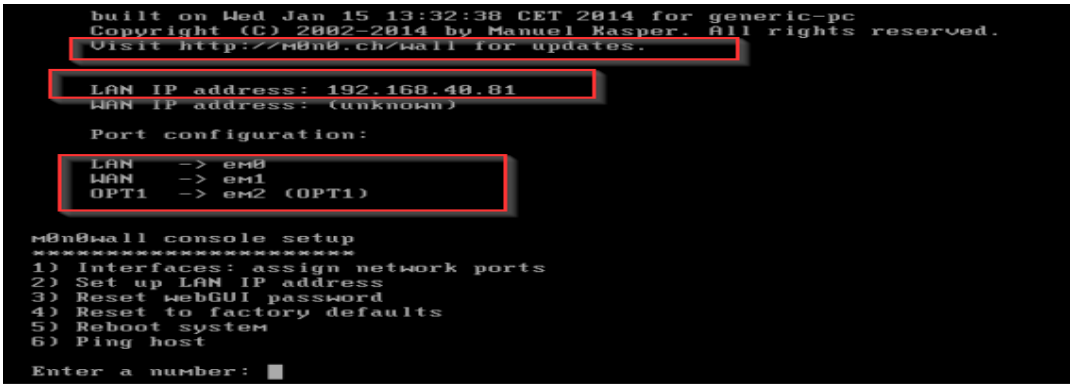


Figura 61. Instalación Monowall
Fuente: Autores

Al momento de configurar y asignar las direcciones IP a cada una de las interfaces podemos gestionar la herramienta al igual que los sistemas anteriores, mediante el acceso web que realizamos desde la VM con Windows 7 presente en el diagrama de red propuesto como se muestra en la figura 62.

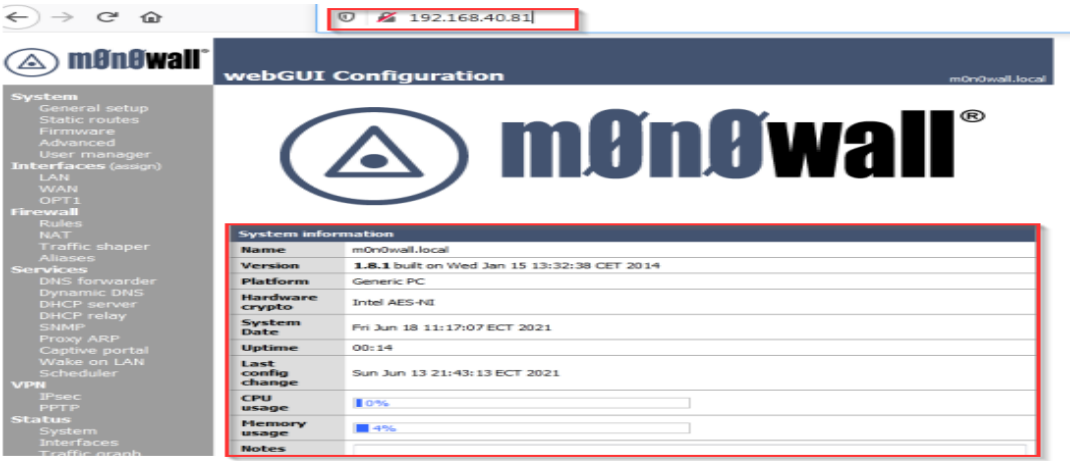


Figura 62. Panel de Control Monowall
Fuente: Autores

La herramienta Monowall al igual que las otras herramientas utilizadas en la presente investigación también es configurada en su escucha o sincronización con el NTP de la red especificado anteriormente como se muestra en la figura 63.

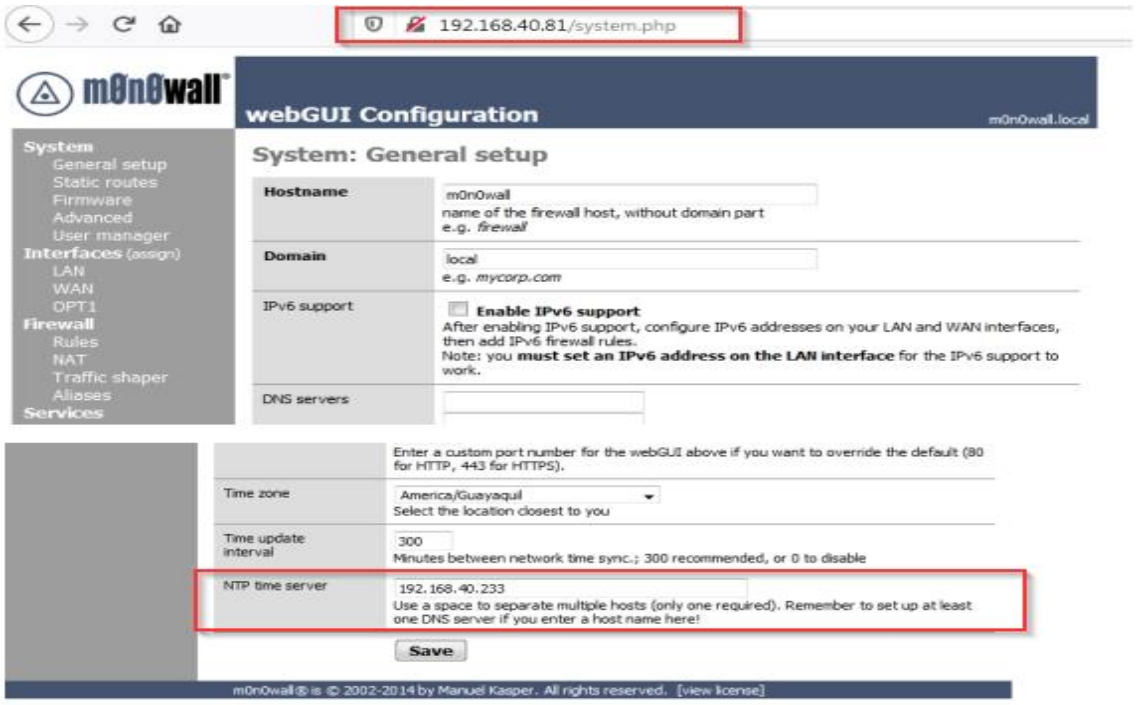


Figura 63. Panel de Control Monowall
Fuente: Autores

Así mismo configuramos el puerto o dirección de escucha donde serán almacenados los logs o eventos generados por el presente dispositivo, esto se realiza mediante la interfaz de escucha configurada en la herramienta AlienVault de OSSIM la misma que ha sido utilizada en cada uno de los dispositivos del presente diagrama de red como se observa en la figura 64.

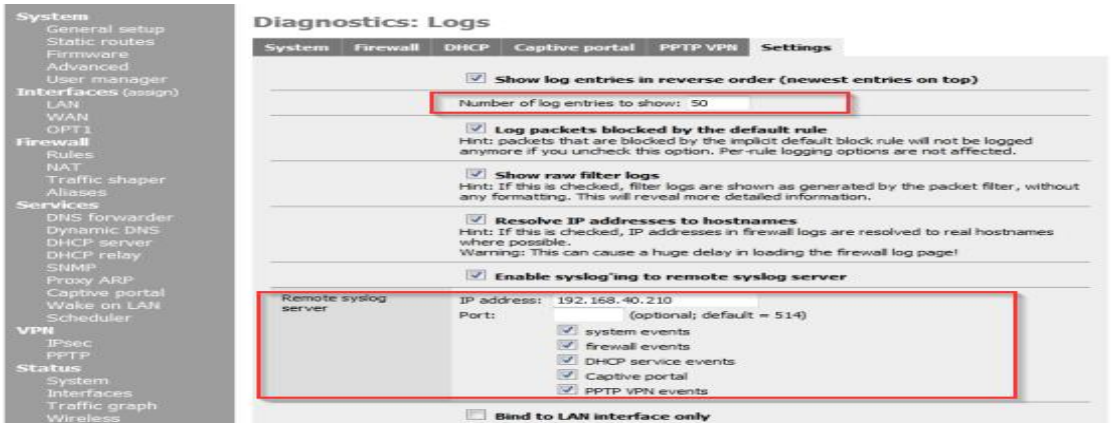


Figura 64. Configuración almacenamiento de logs

Fuente: Autores

En la siguiente gráfica se observa la gestión de los logs o eventos que genera este dispositivo, el mismo que se observa es bastante extenso, aquí se presenta la importancia de contar con una herramienta que haga posible el análisis de todos los eventos generados o detectados en la red, ejemplo de eventos en figura 65.

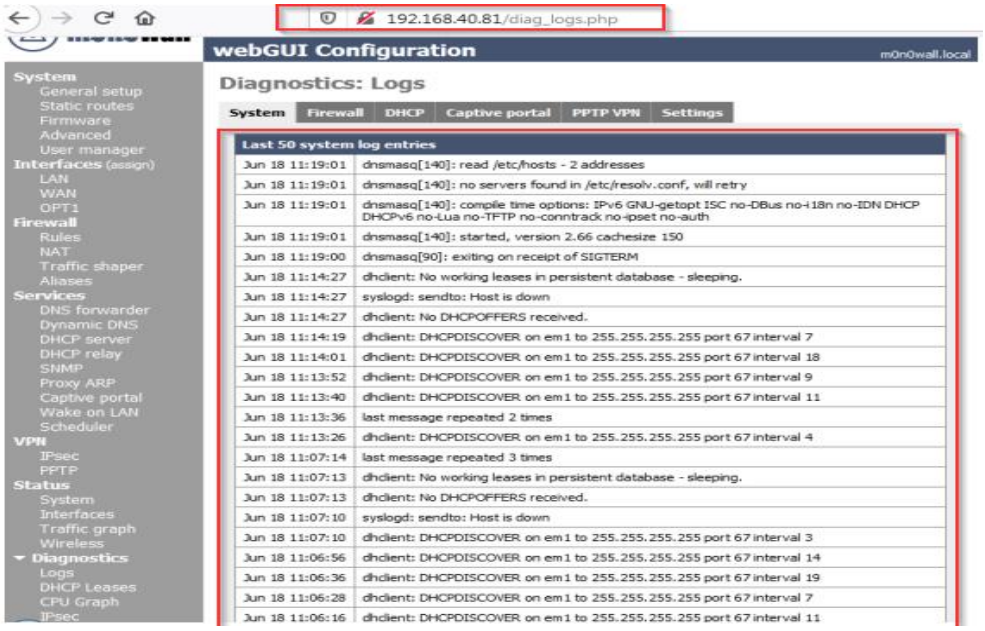


Figura 65. Diagnósticos de Logs entrantes
Fuente: Autores

- **ALIENTVAULT OSSIM**

Continuando con la instalación y configuración de los diferentes componentes que intervienen en la presente propuesta de investigación, procedemos a configurar la máquina virtual para la herramienta OSSIM, quizá la máquina principal dentro de la propuesta de red, pues es quien nos permitirá correlacionar todos la data y ejecutar las políticas asignadas.

Así como gestionar los diferentes perfiles y toma de decisiones de acuerdo al análisis que desempeñe dentro de la red, se muestra la figura 43 con el resumen de la configuración de la VM.

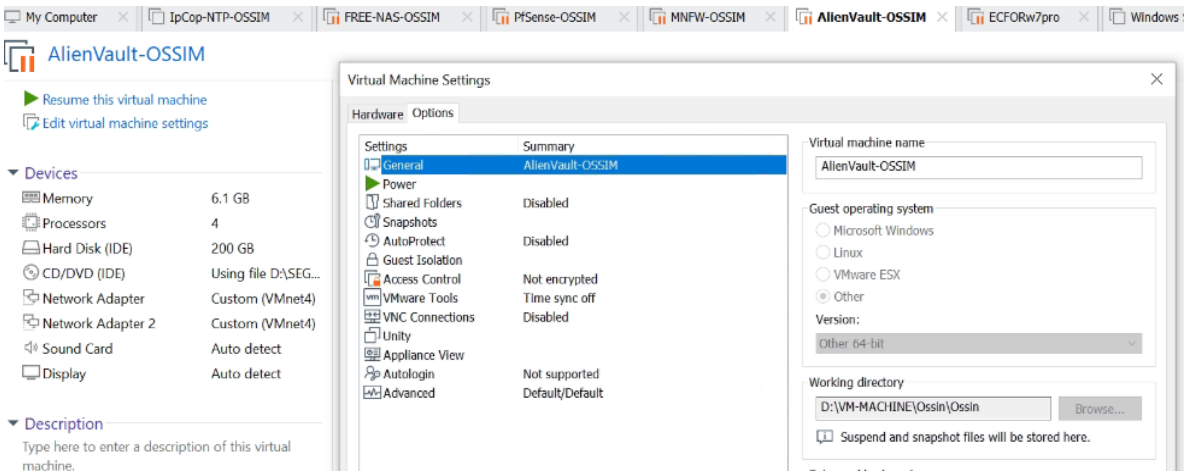


Figura 66. Configuración VM OSSIM
Fuente: Autores

La herramienta OSSIM a manejar en la actual investigación es AlienVault, esta aplicación nos permite la instalación en dos perfiles, servidor y sensor, en el modo servidor se cuenta con las funciones de MONITOR, SENSOR e INTERFAZ GRÁFICA, la segunda el modo sensor estará alerta a las anomalías presentadas en los dispositivos dentro de la infraestructura de red recolectando los log generador por dichos dispositivos, esto a través de agentes instalados en los equipos.

Mediante la consola grafica mostrara todos los eventos suscitados en la red, sean estos captados por un sensor o un monitor, la gestión es mediante un navegador web, en dicha interfaz encontramos varias herramientas como: Nagios, Nmap entre otras. Al comenzar la instalación será necesario especificar la dirección IP para administrar, observamos lo señalado en la figura 67.

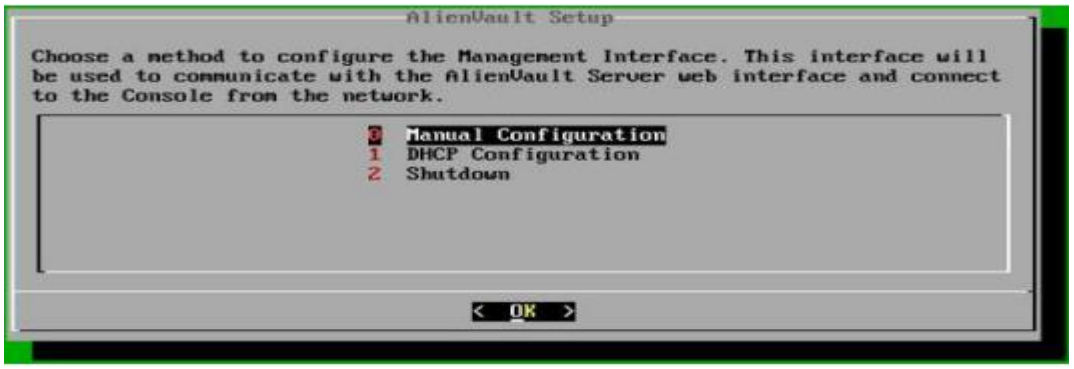


Figura 67. Configuración de la interfaz de administración
Fuente: Autores

Debemos configurar el NTP Server pues de esta manera tendremos sincronizados todos los dispositivos que intervienen en la topología de red señalada, por ende todos los logs que se recopilaran estarán sincronizados, mostramos lo dicho en la figura 68 y 69.

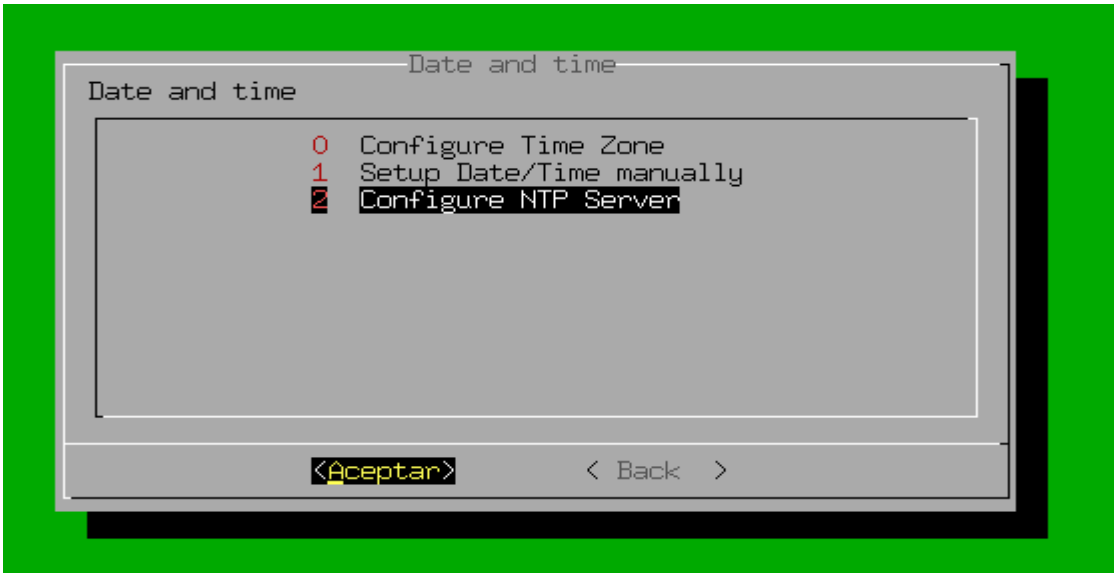


Figura 68. Configuración de NTP Server
Fuente: Autores

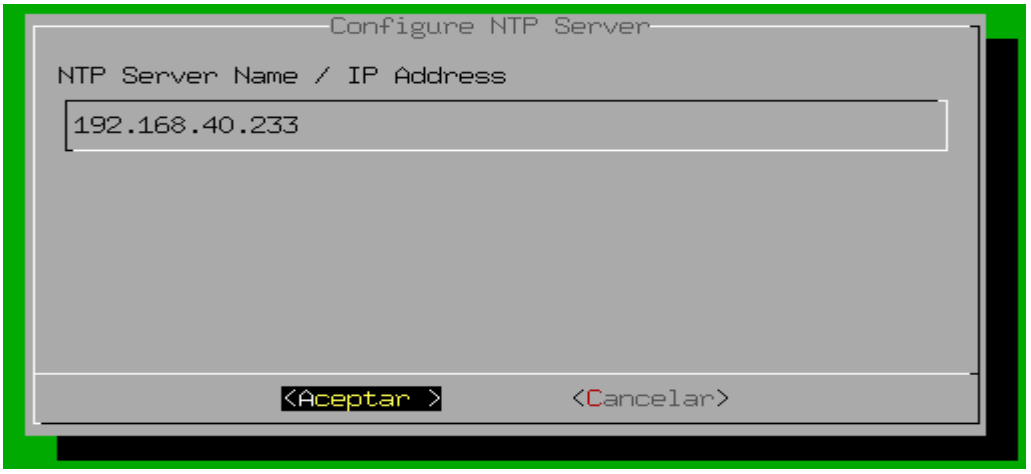


Figura 69. IP del NTP Server
Fuente: Autores

La zona horaria va relacionada con el NTP Server para estar sincronizados con el horario local se muestra figura 70.

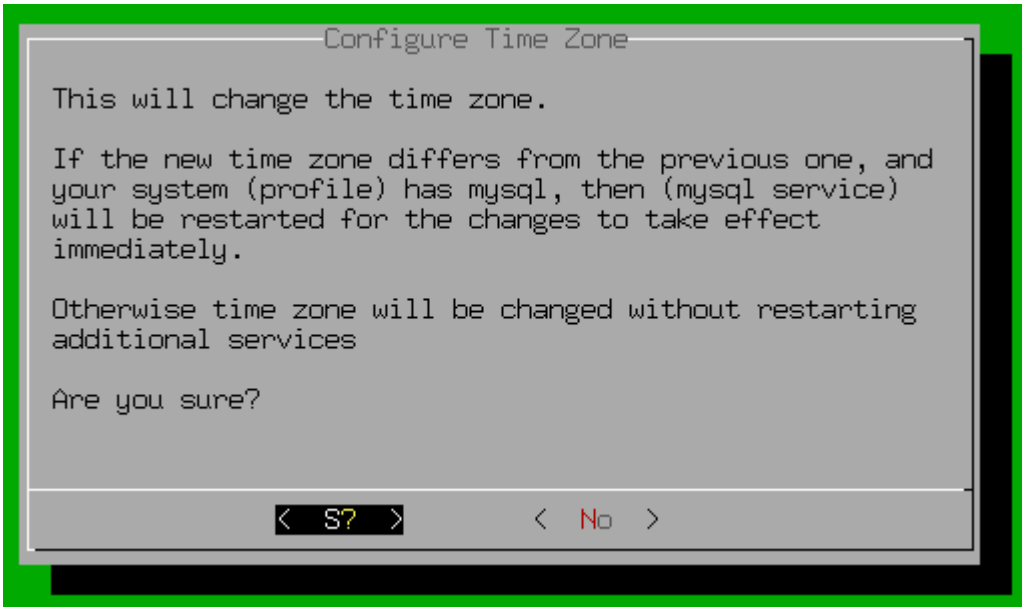


Figura 70. Configuración de la Zona horaria
Fuente: Autores

Aplicamos todos los cambios realizados anteriormente para seguir con la configuración del AlienVault OSSIM como se observa en la figura 71 y 72.

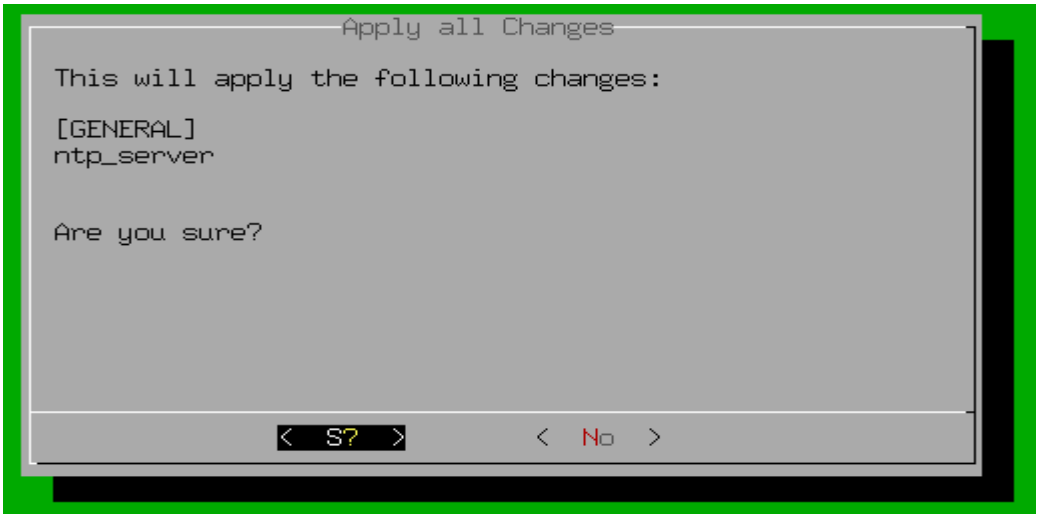


Figura 71. Aplicación de cambios
Fuente: Autores

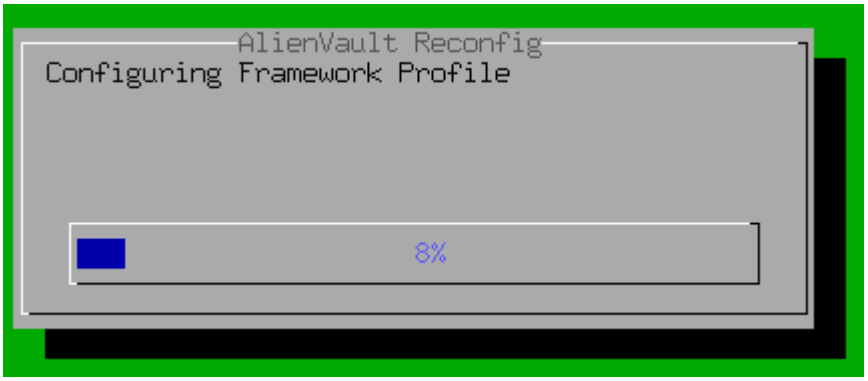


Figura 72. Configuración del Framework
Fuente: Autores

Se configura el Framework de AlienVault para la culminación de la instalación, mostramos la asignación de las interfaces de la herramienta en la figura 73.

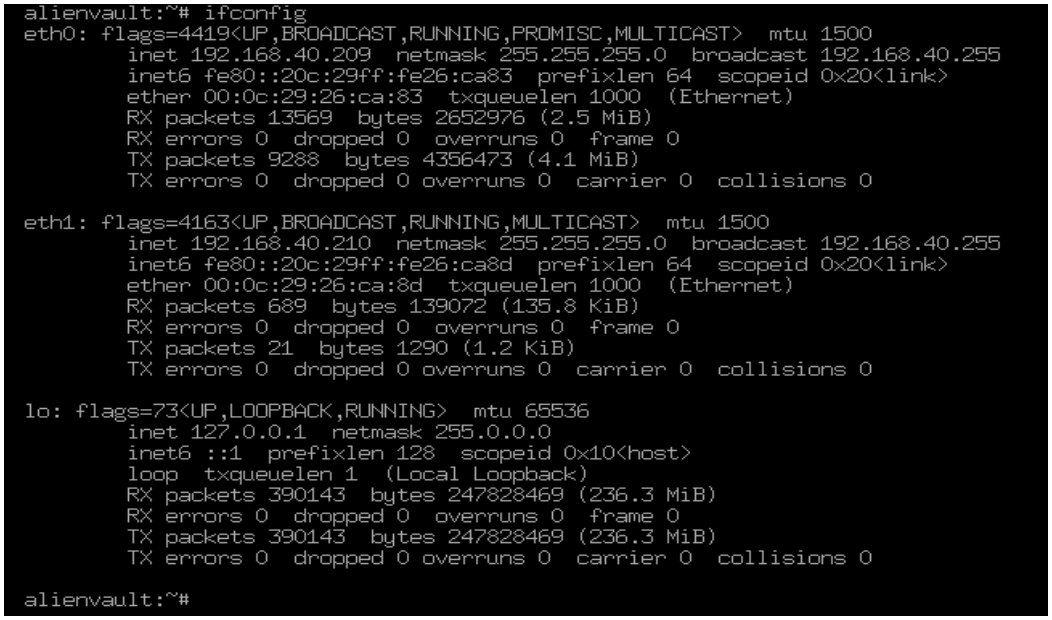


Figura 73. Interfaces de red eth0, eth1
Fuente: Autores

Al culminar la instalación del correlacionar de eventos se ingresara vía web para la gestión de la herramienta, podemos especificar datos como contraseña, emails, responsable de tics entre otros se observa lo anteriormente descrito en la figura 74.

Figura 74. Configuración de credenciales administrativas

Fuente: Autores

Al estar configuradas las credenciales de acceso se procederá a reiniciar el sistema y acceder con las credenciales definidas, ver figura 75.

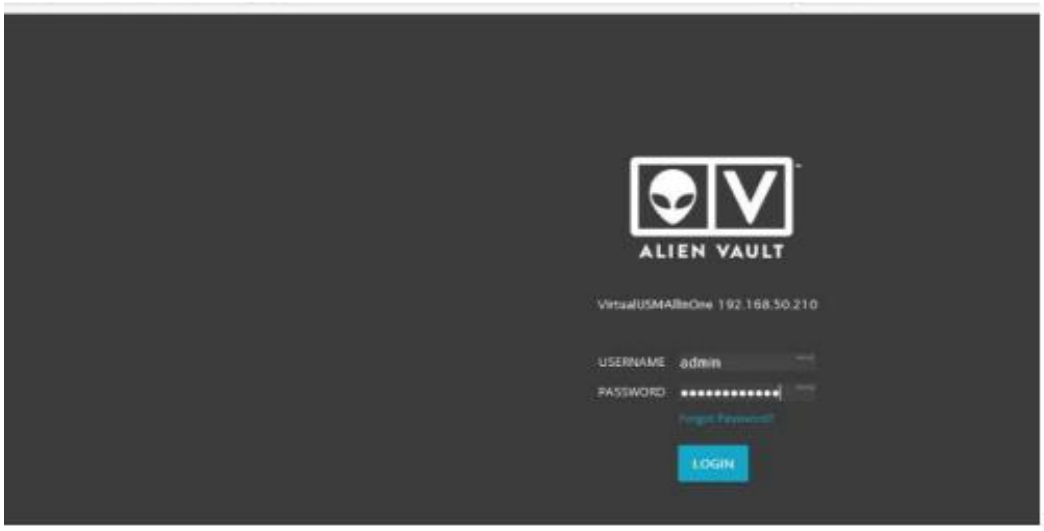


Figura 75. Acceso web al sistema de Correlación de Eventos

Fuente: Autores

En la figura 76 se visualiza el despliegue inicial donde se puede configurar la IP de gestión y de monitoreo, el descubrimiento de los nodos posteriormente colección de logs y monitoreo, alarmas y actividad sospechosa

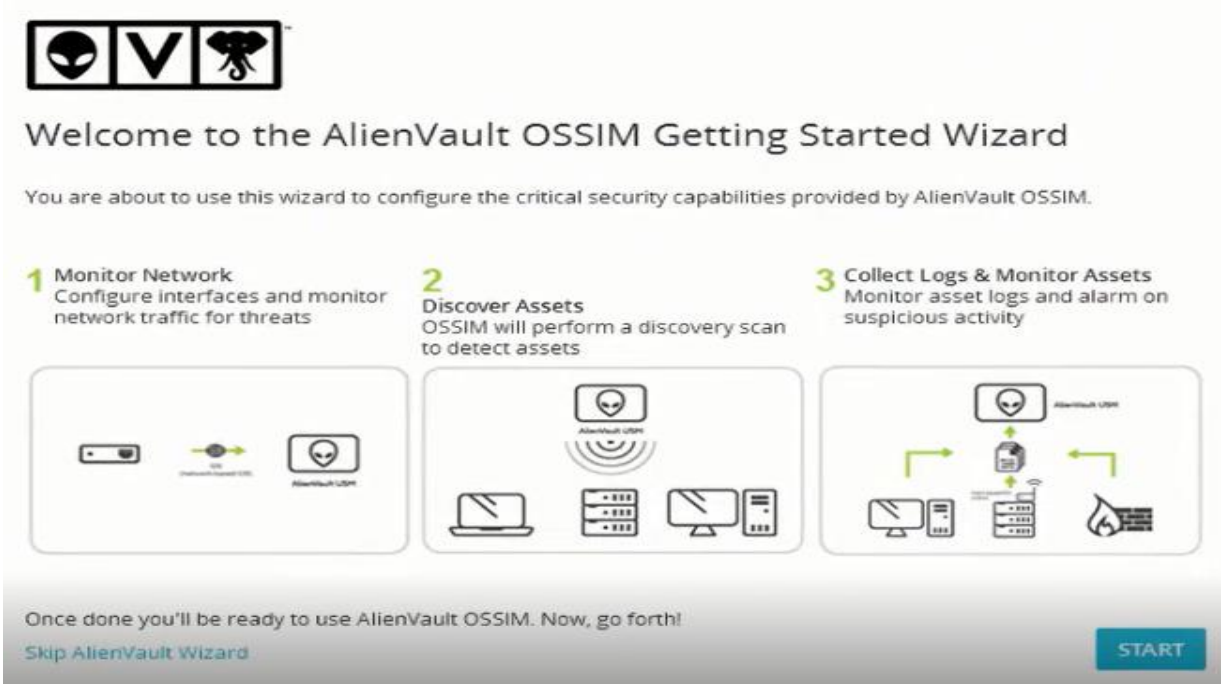


Figura 76 Despliegue Inicial AlienVault OSSIM
Fuente: Autores

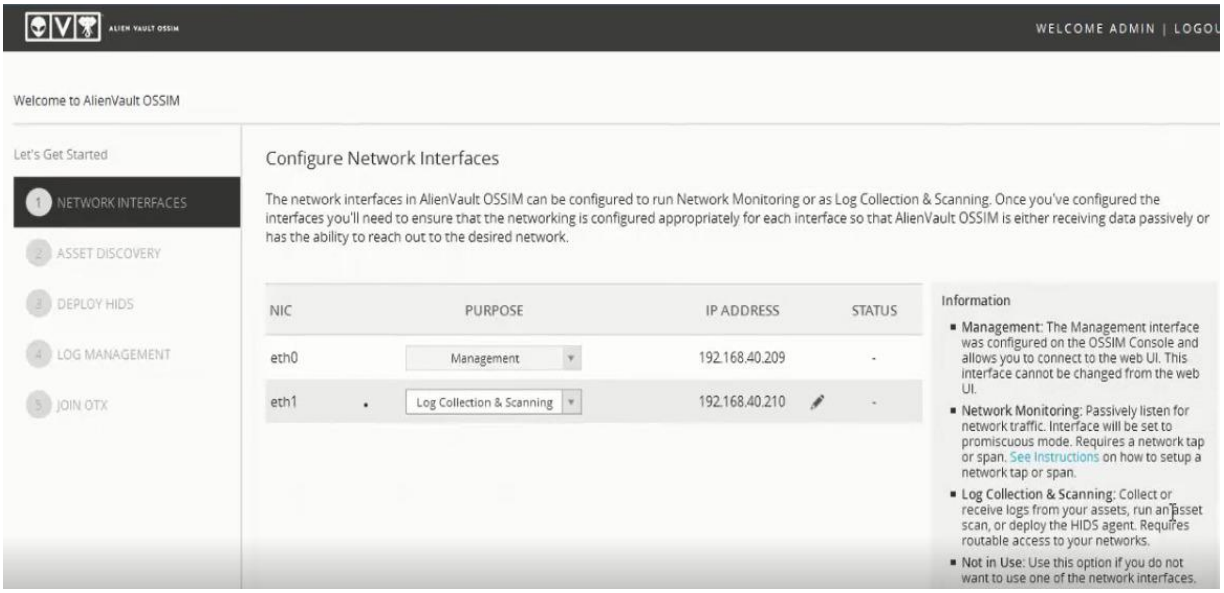


Figura 77 Configuración de interfaces de gestión y colección de logs
Fuente: Autores

Descubrimiento de nodos barre la red 192.168.40.0 va a descubrir los nodos Pfsense, FreeNas, Monowall, Windows Server, Windows 7.

A continuación especificamos el tipo de interfaz y la característica de gestión previamente definida ver figura 78.

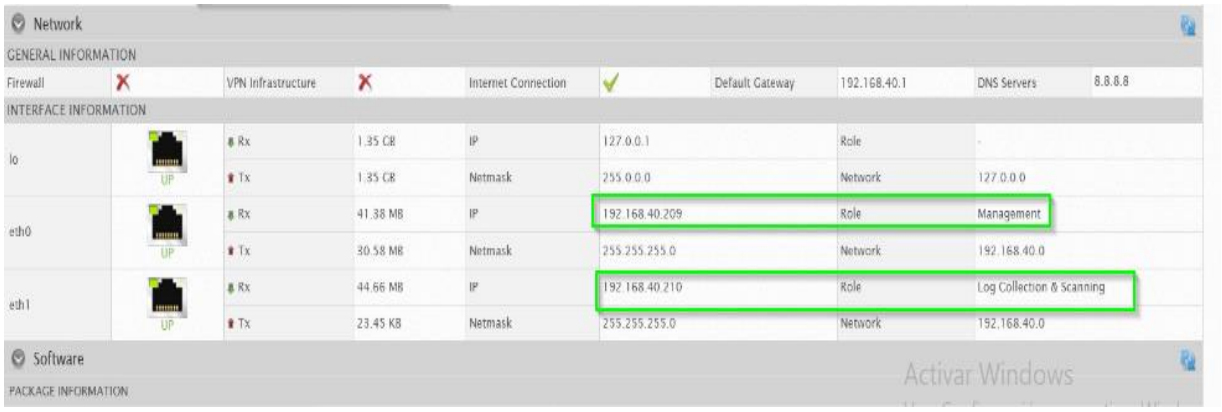


Figura 78. Interfaces de Red, funcionalidad y modo de la interfaz.

Fuente: Autores

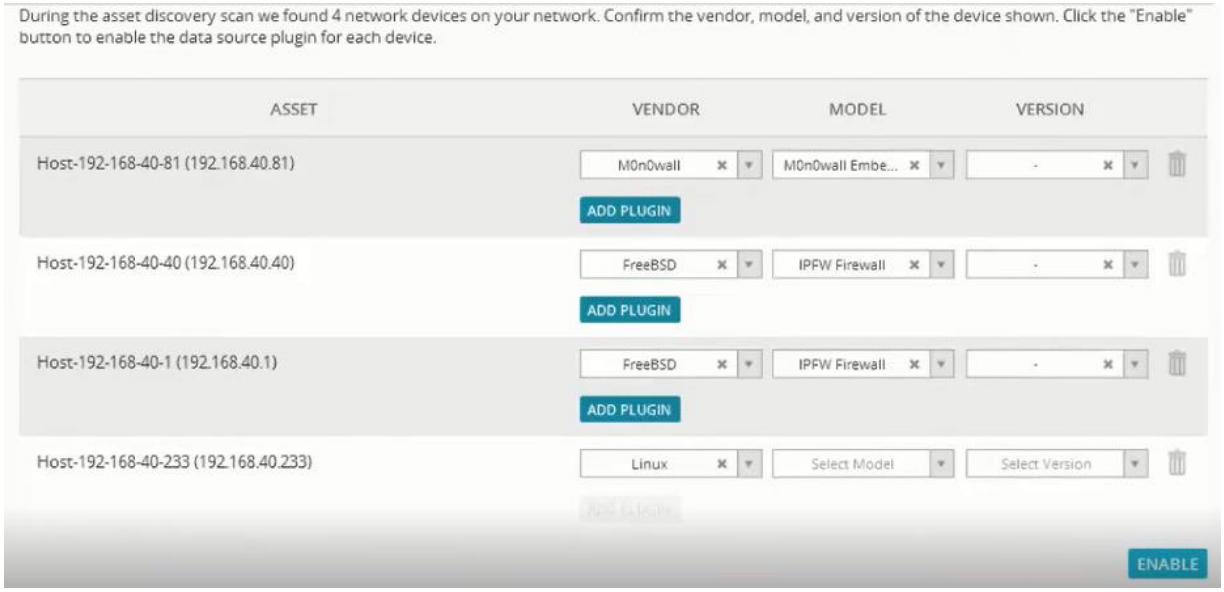


Figura 79 Habilitación de plugins
Fuente: Autores

Tenemos la parte de habilitación de plugins para cada una de los dispositivos que van a interactuar con el OSSIM

- **CONFIGURACIÓN DE LAS REGLAS PARA LA CORRELACIÓN DE EVENTOS**

Al configurar los orígenes de datos, es necesario determinar las reglas de correlación, teniendo en cuenta el habilitar un colectar por cada dispositivo que deseamos monitorear, se deben tener en cuenta las rutas a configurar al habilitar los colectores.

Tabla 12 Principales rutas de configuración OSSIM

Ruta del archivo de configuración	Descripción
/etc/ossim/ossim_setup.conf	Archivo de configuración SIEM
/etc/ossim/server/config.xml	Archivo configuración del servidor
/etc/ossim/agent/config.cfg	Archivo configuración de los agentes
/etc/ossim/framework/ossim.conf	Archivo configuración de interfaz y base de datos
/etc/mysql/my.cnf	Archivo de configuración base datos
/etc/snort/snort.ethN.conf	Archivo de configuración Snort
/etc/openvas/openvasd.conf	Archivo de configuración OpenVas
/etc/nagios3/	Archivo de configuración Nagios

Fuente: Autores

Dentro del archivo de configuración /etc/ossim/ossim_setup.conf se deberán tener en cuenta los Siguientes parámetros:

Tabla 13 Archivo de configuración Ossim

Parámetro	Descripción
Admin_dns	IP del servidor dns
Admin_gateway	IP del Gateway
Admin_ip	IP de la interfaz de gestión.
Admin_netmask	Mascara de la red de gestión.
Domain	Nombre del dominio ubicación del dispositivo AlienVault
Email_notification	Email para notificaciones
Hostname	Nombre del servidor SIEM.
Interface	Interfaz de gestión.
Mailserver_relay	IP del servidor de correo
Mailserver_relay_passwd	Contraseña del usuario para reenviar correos.
Mailserver_relay_port	Puerto del servidor de correo
Mail server_relay_user	Nombre del usuario para reenviar correos
Ntp_server	IP del servidor NTP.
Profile	Perfil del equipo de AlienVault (Sensor, Server, Framework o Database)
db_ip	IP de la base de datos.
pass	Contraseña de un usuario de la base de datos

user	Usuario para conectarse a la base de datos
Active	Activar o desactivar el firewall de AlienVault
Framework_https_cert	Ruta para el certificado de la consola
webFramework_https_key	Ruta para la clave privada del certificado
Framework_ip	IP de la consola web.
Detectors	Plugins del tipo detector habilitados en el sensor.
Interfaces	Interfaces que están en modo promiscuo
ip	IP del Sensor.
monitors	Plugins del tipo monitor habilitados en el sensor.
name	Nombre del Sensor.
networks	Rangos de las redes a monitorizar.
tzone	Zona horaria del Sensor.
server_ip	IP del Server (USM y/o Logger).
update_proxy	Activar el uso de un proxy.
update_proxy_dns	Dirección del proxy.
update_proxy_pass	Contraseña del usuario para conectarse al proxy.
update_proxy_port	Puerta para conectarse al proxy.
update_proxy_user	Usuario para conectarse al proxy.

vpn_infraestructure	Habilitar las configuraciones para la VPN
vpn_net	Red de la VPN
vpn_netmask	Mascara de red para la VPN.

Fuente: Autores

ANEXO 2. FASE DE OPERACIÓN

En la fase de operación se pretende visualizar varias de las funcionalidades y prestaciones que presenta la herramienta AlienVault OSSIM entre las cuales mencionamos IDS, análisis de vulnerabilidades, alertas, ticket entre otros. De igual manera se observar la funcionalidad de las diferentes herramientas que intervienen en la infraestructura de red propuesta.

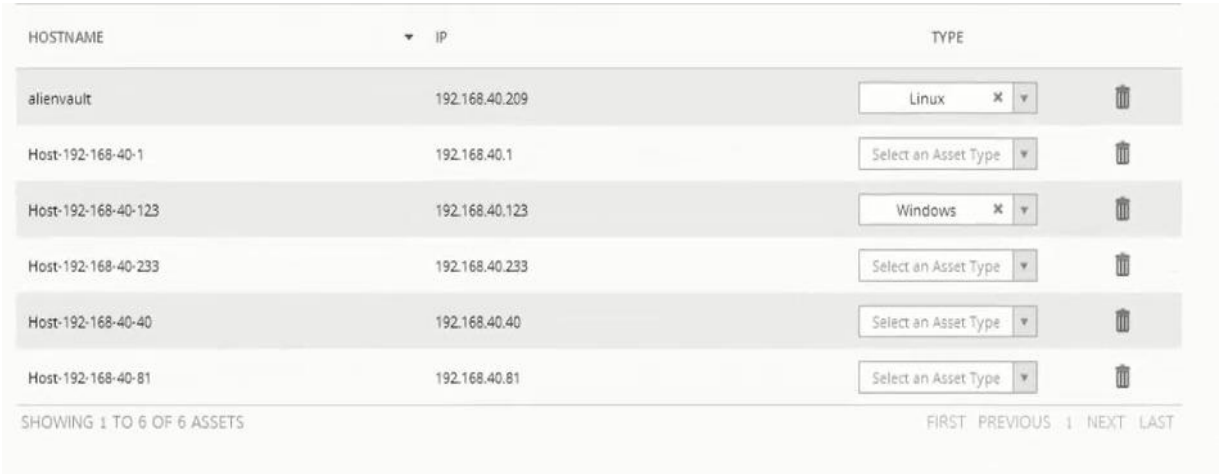


Figura 80. Dispositivos y sistemas operativos especificados
Fuente: Autores

Una vez realizado el proceso anterior se debe especificar el tipo de S.O de los clientes anteriormente identificados en el escaneo, para esto se utiliza la técnica Ping Sweep, en caso que un dispositivos no responda solicitudes ICMP podrá ser agregado manualmente.

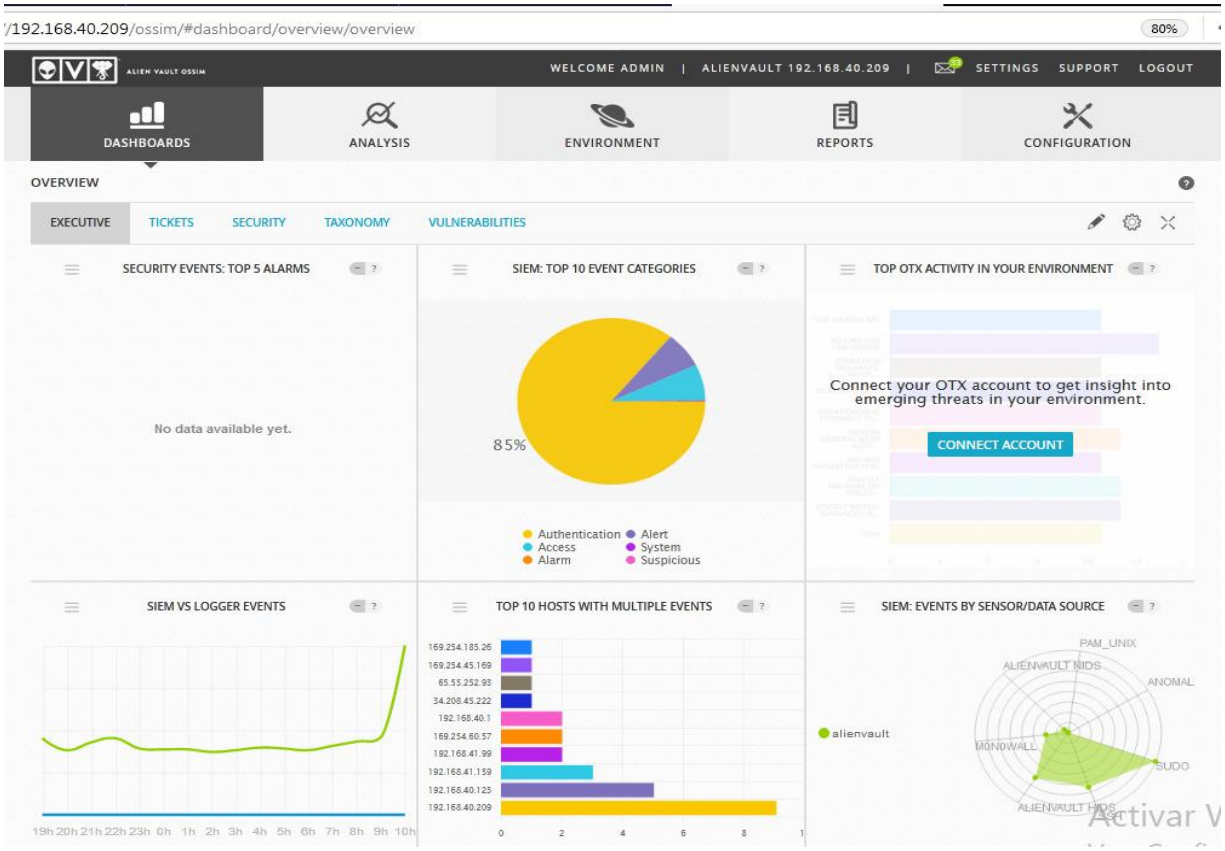


Figura 81. Panel de Control AlienVault OSSIM
Fuente: Autores

En la figura 81 se observa el panel de control que tiene AlienVault Ossim, en el cual se visualizan alarmas, eventos, hosts con más eventos múltiples, y demás opciones que nos da la herramienta.

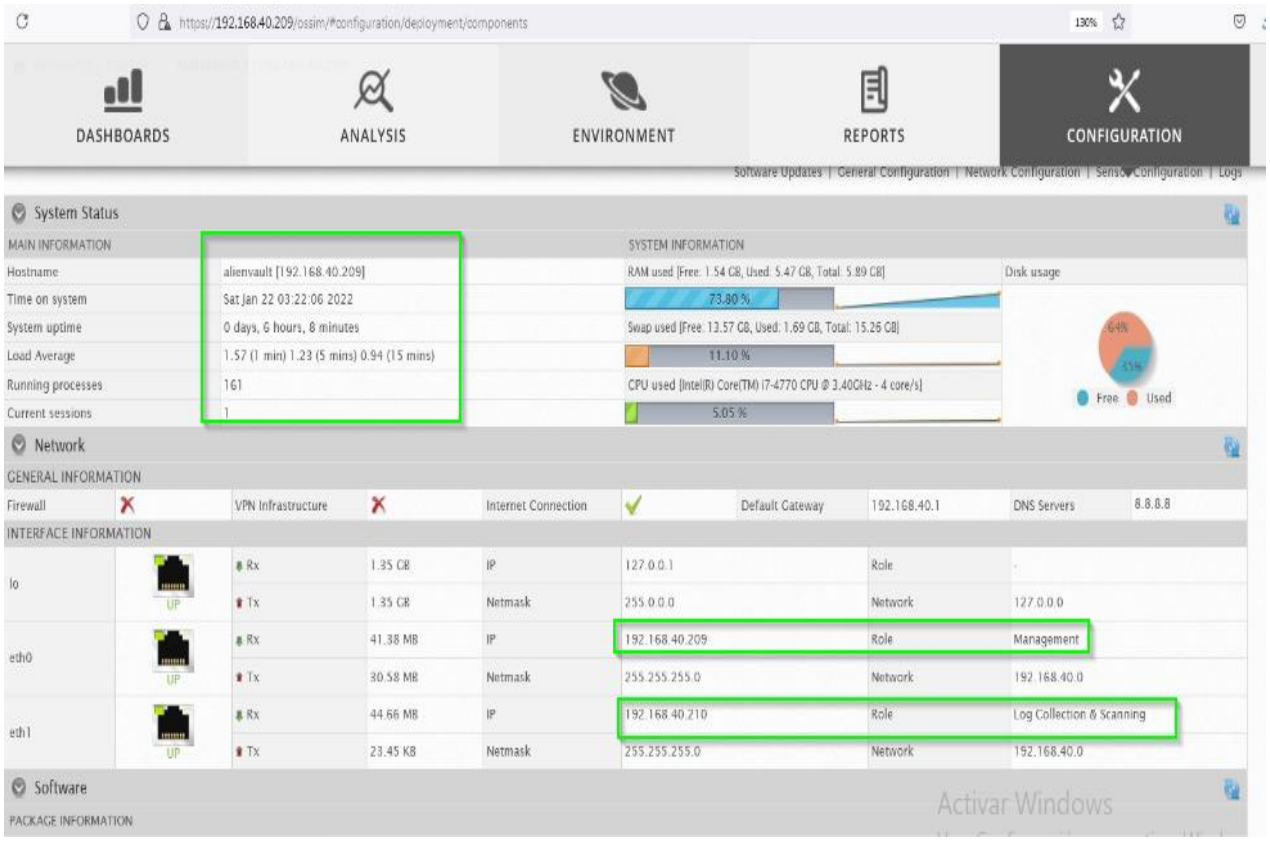


Figura 82. Configuración General de AlienVault OSSIM
Fuente: Autores

En la figura 82 se visualiza el estado del sistema y sus distintas configuraciones, así como el uso de memoria RAM y uso de almacenamiento, las interfaces que están habilitadas, la versión del software y demás información proporcionada por la herramienta.

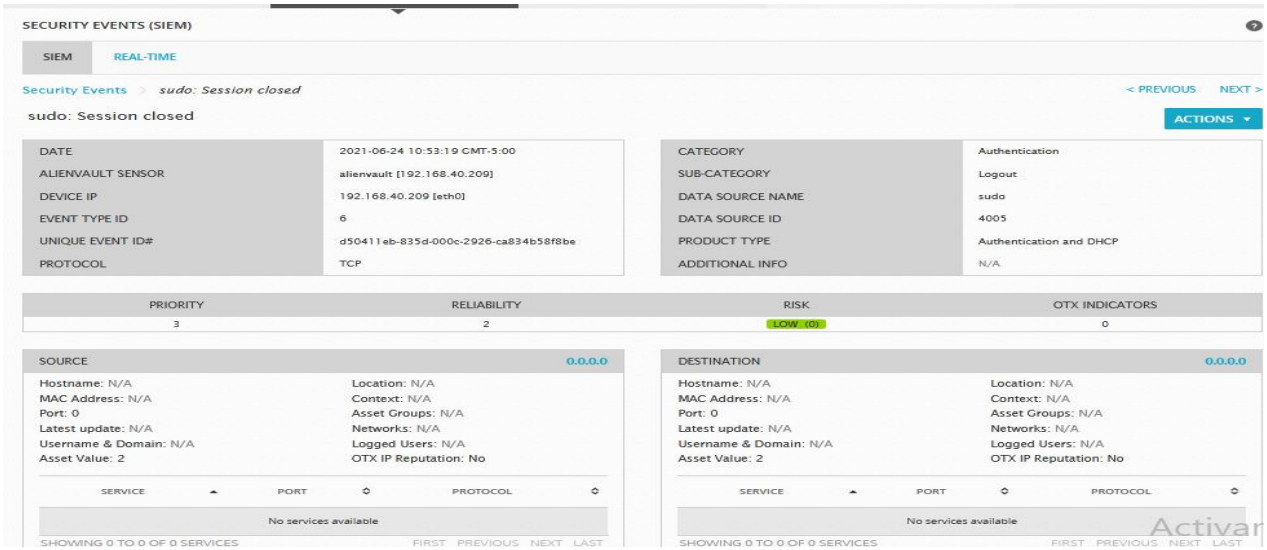


Figura 83. IDS
Fuente: Autores

En la figura 83 se evidencia la colección de un evento de seguridad, donde se observa el inicio de sesión no autorizado registrado por la herramienta AlienVault OSSIM, así mismo se visualiza el tipo de evento, la prioridad, el riesgo y demás información generada.

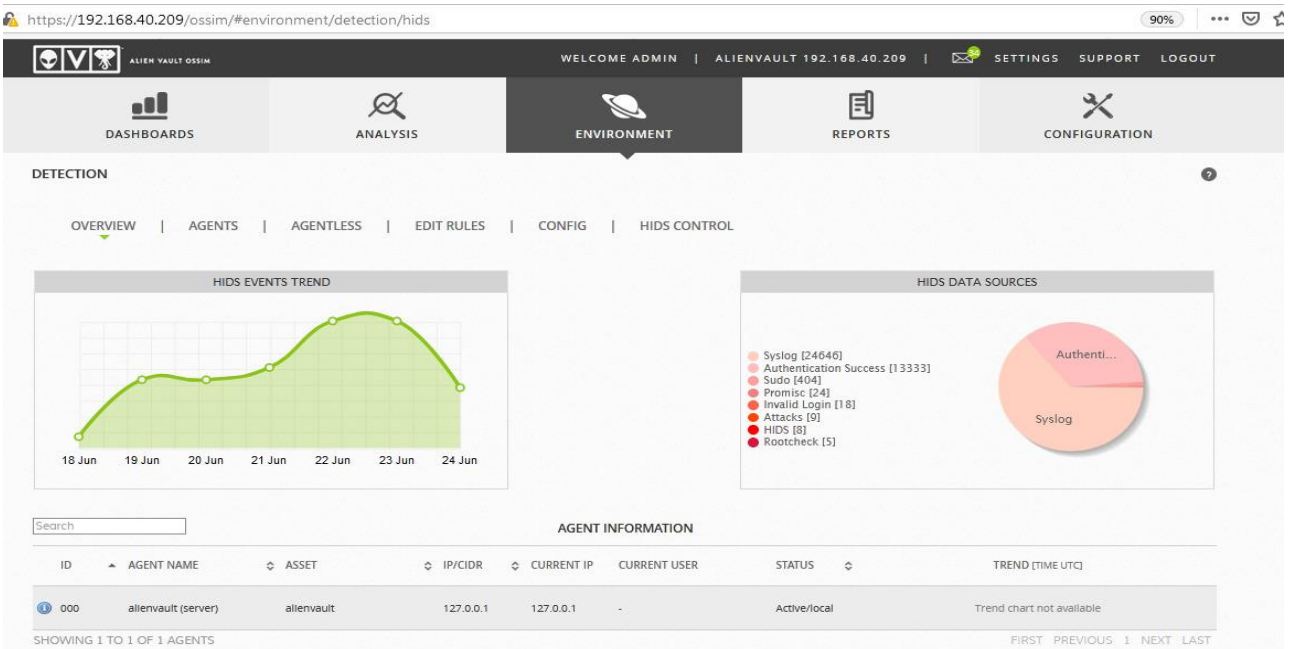


Figura 84. HIDS Eventos
Fuente: Autores

Se puede observar una detección de intrusos a nivel de host HIDS (Sistema de Detector de Intrusos Host), donde se muestra una estadística de tendencias de los eventos, y como se han recibido ya sea estos de autenticación o Syslog.

Figura 85. Netflow Monitoreo
Fuente: Autores

Tenemos una vista del monitorio de tráfico de red que permite visualizar el comportamiento de un host o una red, así como el tráfico generado por protocolos TCP, UDP, ICMP y otros, como también los paquetes recibidos y la afluencia de los mismos en un tiempo determinado.

Figura 86. NTOP
Fuente: Autores

En la figura 86 se visualiza el monitoreo de red mediante la herramienta Ntop, en el cual se puede apreciar el flujo de estos desde distintas direcciones ip, como también del FW Pfsense.

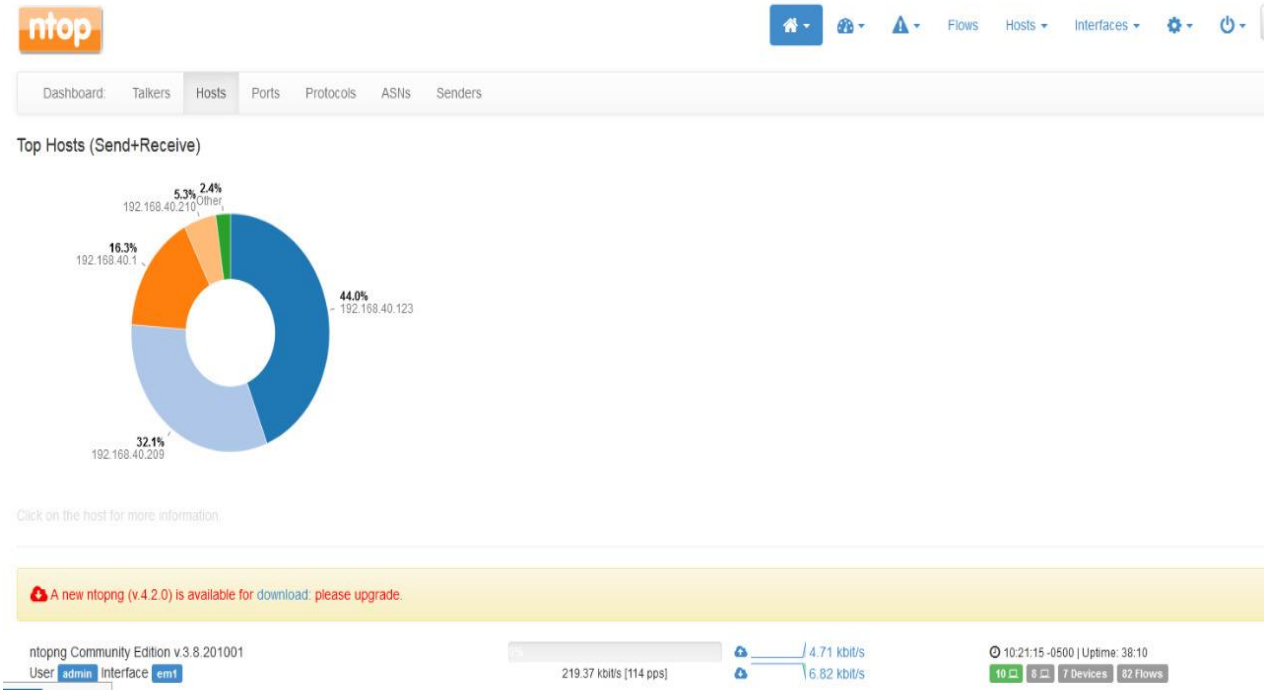


Figura 87. NTOP Numero de host
Fuente: Autores

Una estadística de los host que envían y reciben tráfico en la red la cual nos genera la herramienta Ntop, se observa la IP 192.168.40.123 correspondiente a Windows 7 tiene el mayor porcentaje de tráfico, le sigue la IP 192.168.40.209 que corresponde al AlienVault Ossim y la IP 192.168.40.1 siendo el Pfsense entre los que hay más afluencia de tráfico en la red, para darnos cuenta desde donde se ha generado más afluencia de tráfico el cual se muestra en forma de porcentaje indicando un color para cada host analizado.

Tabla 14 Estadísticas de host en NTOP

Host	Porcentaje
192.168.40.123	44%
192.168.40.209	32%
192.168.40.1	16%
192.168.40.240	5%
other	3%

Fuente: Autores

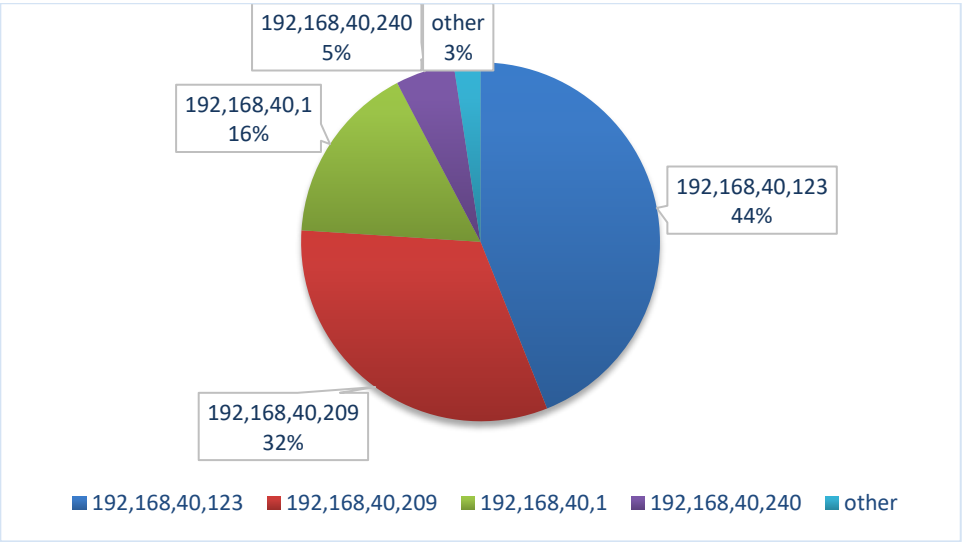


Ilustración 6 Estadísticas de host en NTOP
Fuente: Autores

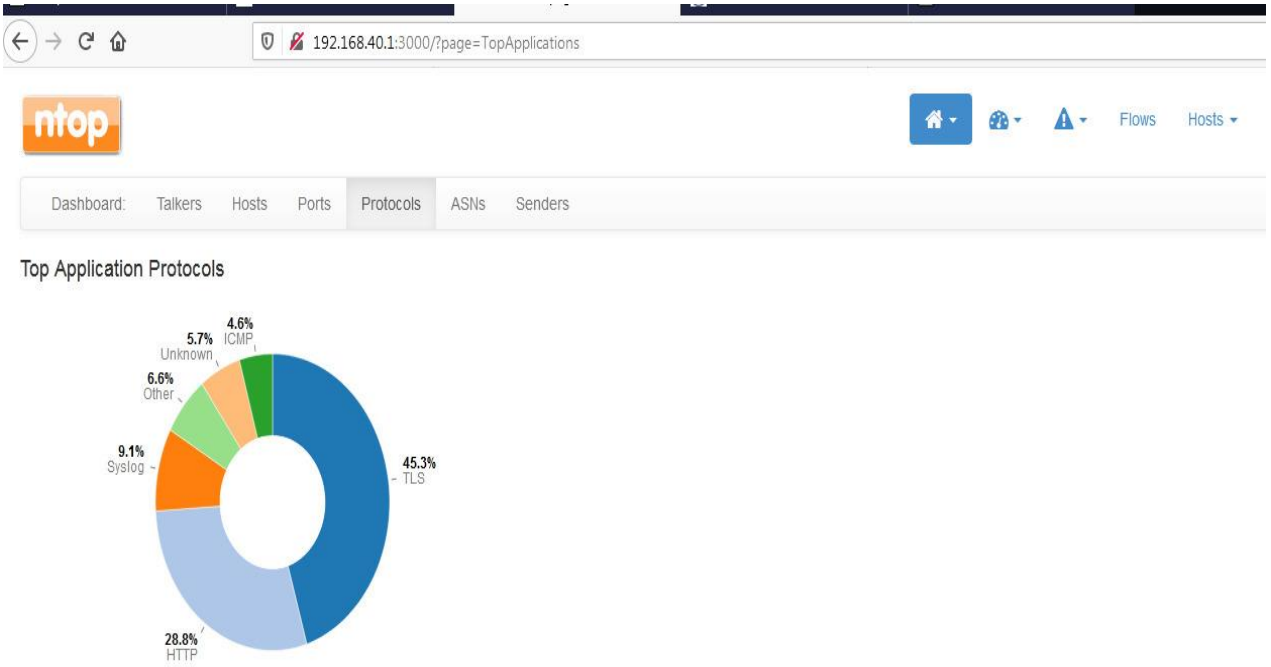


Figura 88. NTOP Protocolos en uso
Fuente: Autores

Así mismo Ntop muestra en la figura 88 un top de aplicación de protocolos más usado en el tráfico de red, siendo el TLS y HTTP los más aplicados de acuerdo la estadística que refleja la herramienta.

Tabla 15 Estadísticas de Protocolos NTOP

Protocolo	Porcentaje
TLS	45.3%
HTTP	28.3%
Syslog	9.1%
Other	6.6%
Unknow	5,7%
ICMP	4.6%

Fuente: Autores

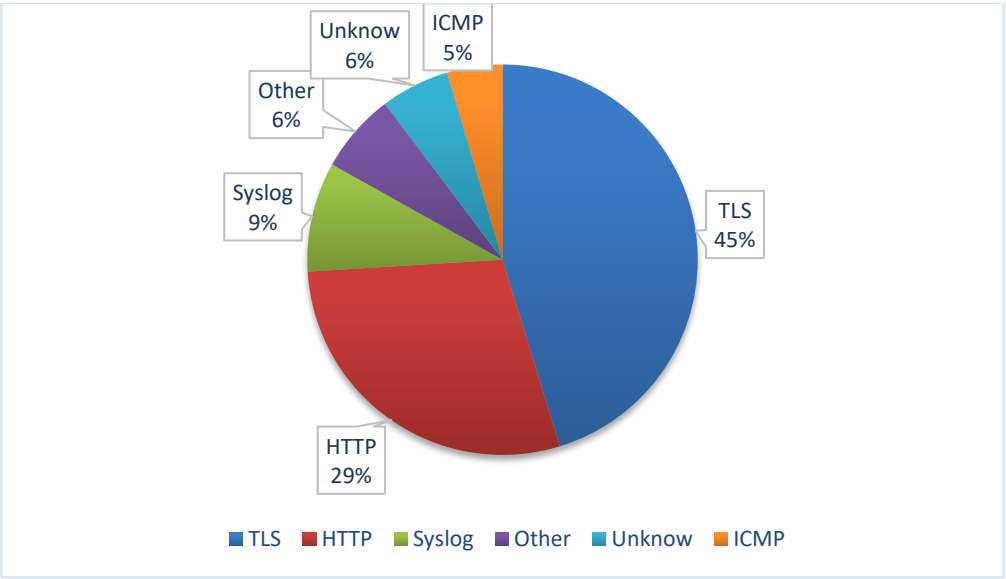


Ilustración 7 Estadísticas de Protocolos NTOP
Fuente: Autores

En la figura 89 se observa un análisis de vulnerabilidad realizado por la herramienta SIEM, permitiendo obtener la cantidad de vulnerabilidades encontradas en dichos nodos.

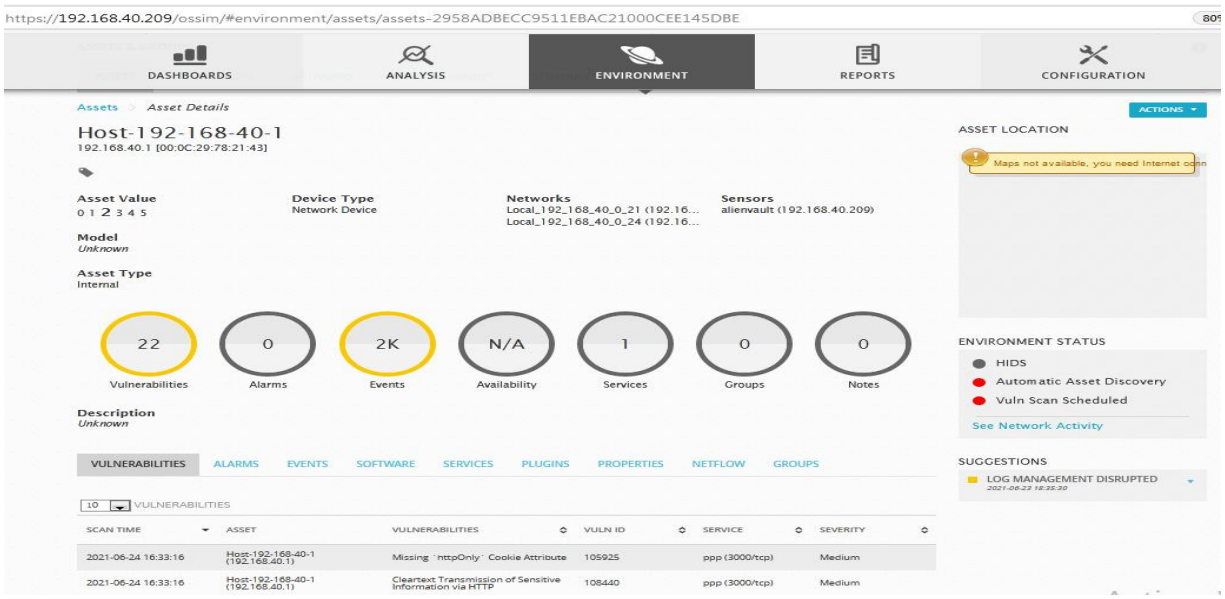
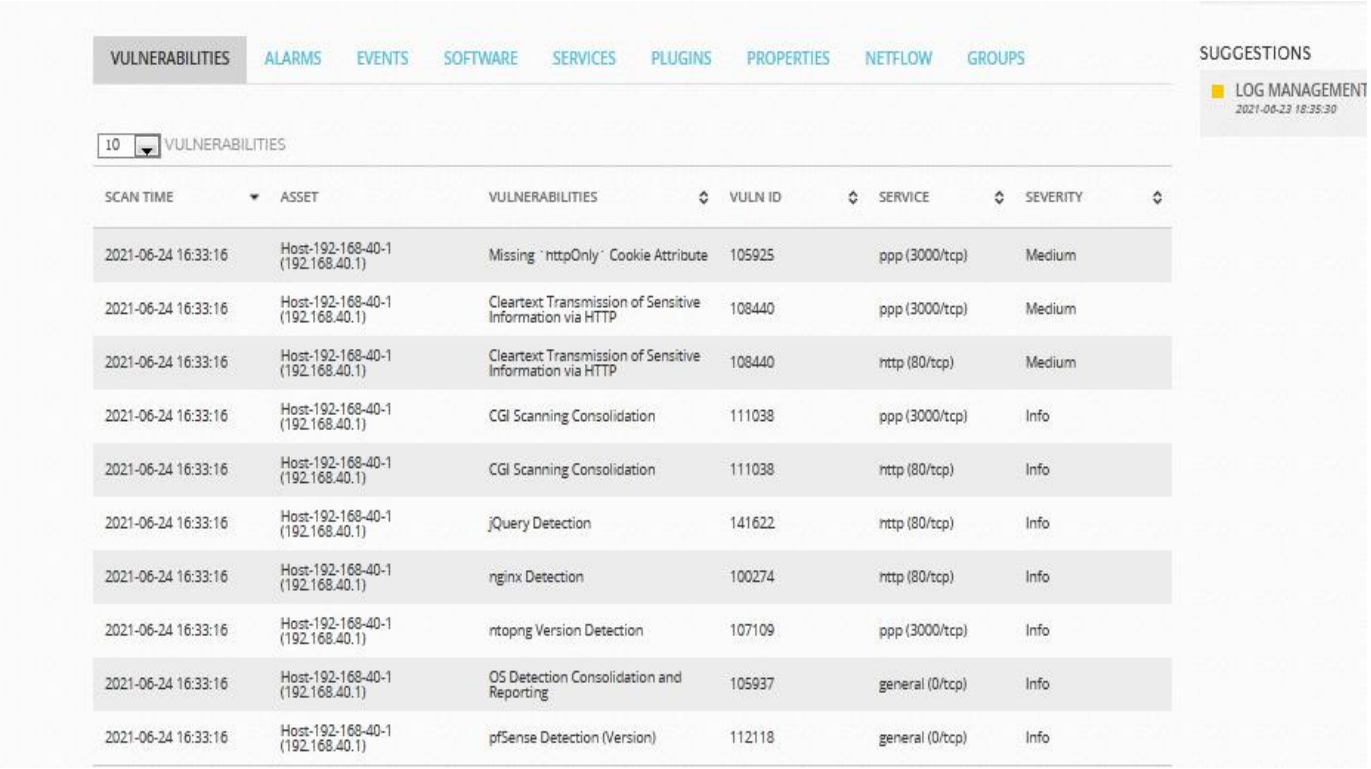


Figura 89. Análisis Vulnerabilidades
Fuente: Autores



SCAN TIME	ASSET	VULNERABILITIES	VULN ID	SERVICE	SEVERITY
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	Missing 'httpOnly' Cookie Attribute	105925	ppp (3000/tcp)	Medium
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	Cleartext Transmission of Sensitive Information via HTTP	108440	ppp (3000/tcp)	Medium
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	Cleartext Transmission of Sensitive Information via HTTP	108440	http (80/tcp)	Medium
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	CGI Scanning Consolidation	111038	ppp (3000/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	CGI Scanning Consolidation	111038	http (80/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	jQuery Detection	141622	http (80/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	nginx Detection	100274	http (80/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	ntopng Version Detection	107109	ppp (3000/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	OS Detection Consolidation and Reporting	105937	general (0/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	pfSense Detection (Version)	112118	general (0/tcp)	Info

Figura 90. Descripción de Vulnerabilidades
Fuente: Autores

En la figura 90 se visualiza el número y nivel de severidad de las vulnerabilidades, el equipo afectado el cual corresponde al Pfsense con la IP 192.168.40.1, y la descripción de las vulnerabilidades entre las que tenemos nginx Detection, JQuery Detection entre otros.

Podemos visualizar en las siguientes figuras un ataque payload registrado por el SIEM y la herramienta NIDS (Sistema de Detección de Intrusos de Red), que registra también desde donde se originó el ataque (IP origen 192.168.40.123) y cuál fue su destino (IP destino 192.168.40.81), señalando el puerto utilizado, a su vez en las figuras 70 y 71 refleja que el password no está encriptado y las reglas de detección del ataque.

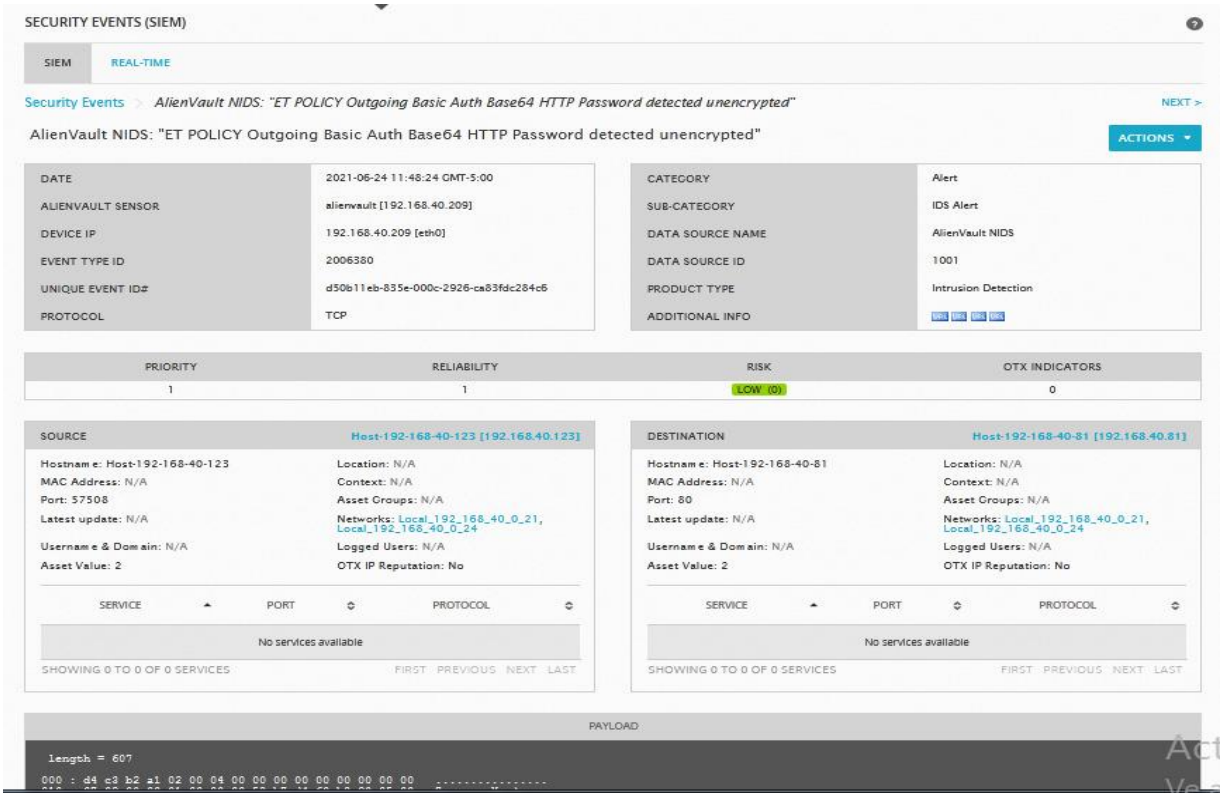


Figura 91. Payload Detectado
Fuente. Autores

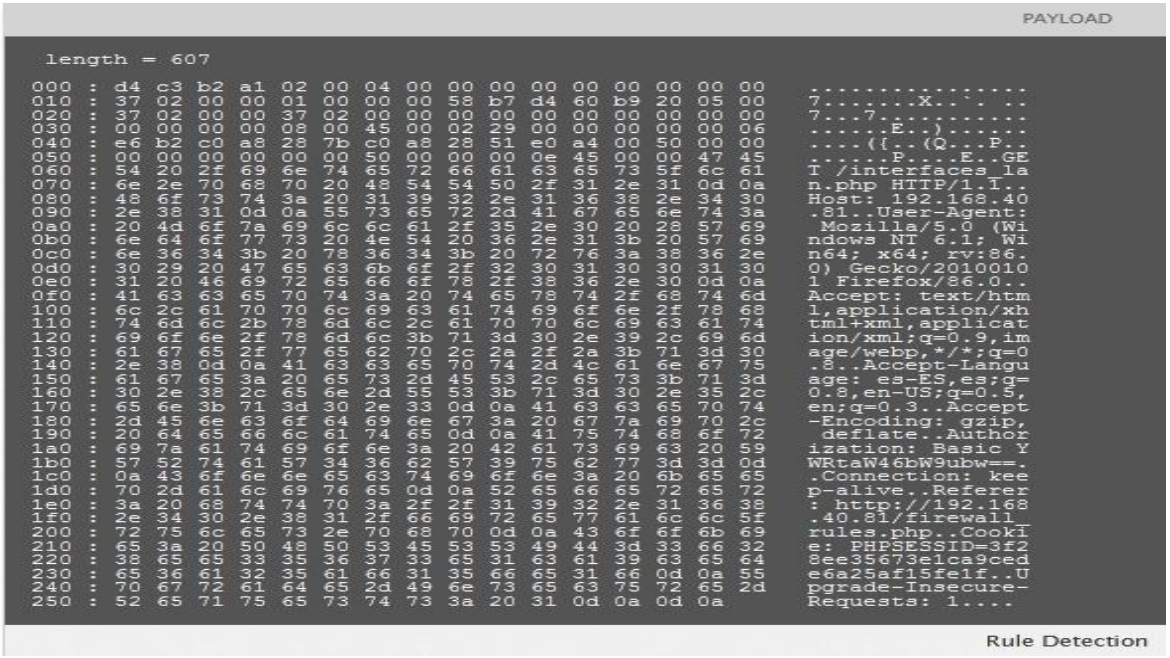


Figura 92. Descripción de Payload
Fuente: Autores

Figura 93. Descripción ataque Payload
Fuente: Autores

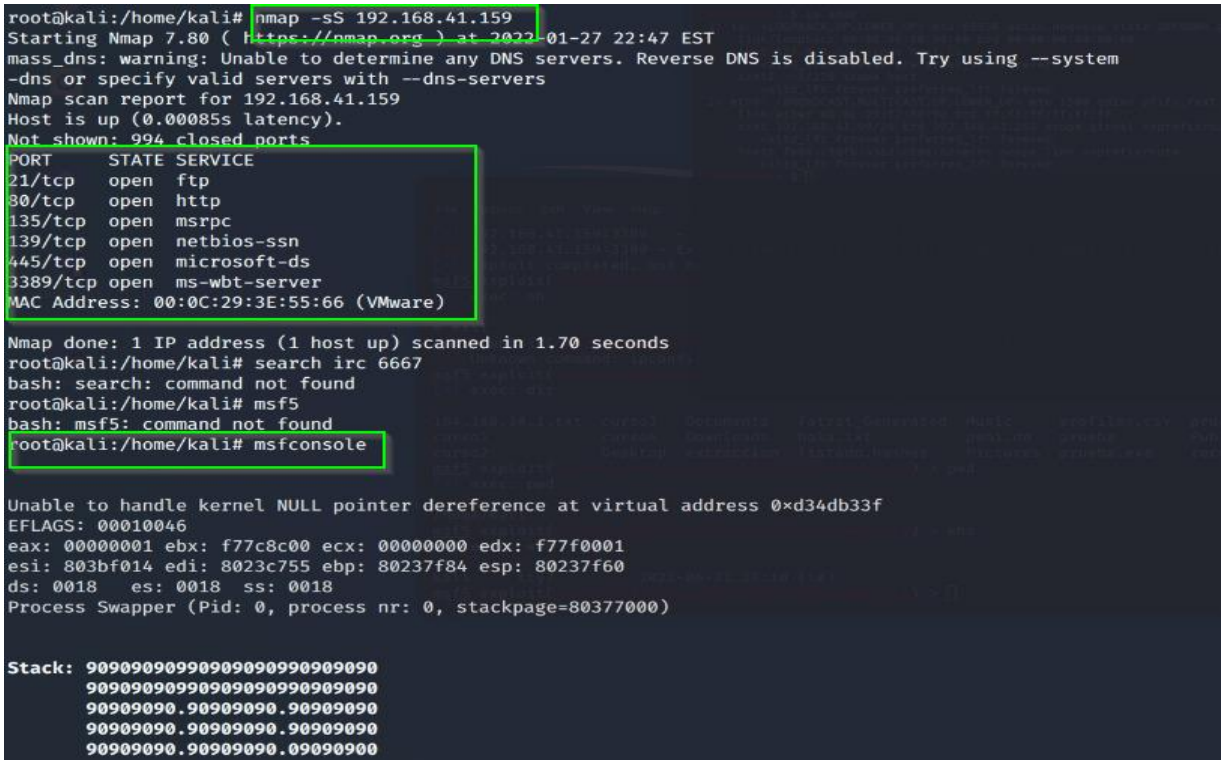


Figura 94. Preparación para ataque Metasploit
Fuente: Autores

Se muestra en la figura 94 que se realiza un escaneo con el comando nmap y la IP 192.168.4.159, en la que se visualiza los puertos abiertos como son el ftp, http, NetBIOS entre otros y procedemos a arrancar el msfconsole.

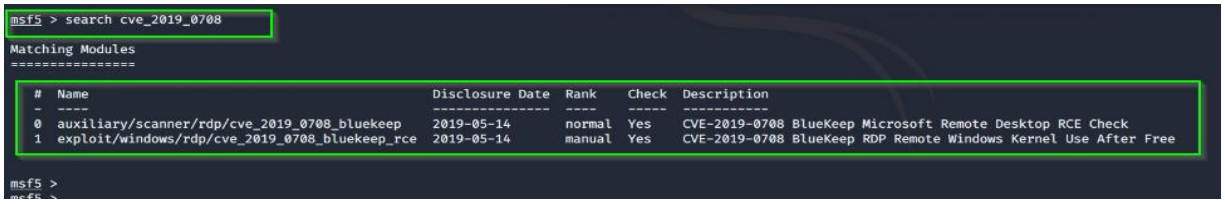


Figura 95. Búsqueda en msfconsole
Fuente: Autores

Se procede a buscar la vulnerabilidad con el comando search y el código para realizar la explotación del escritorio remoto en la que se describe el nombre, el rango y su descripción.

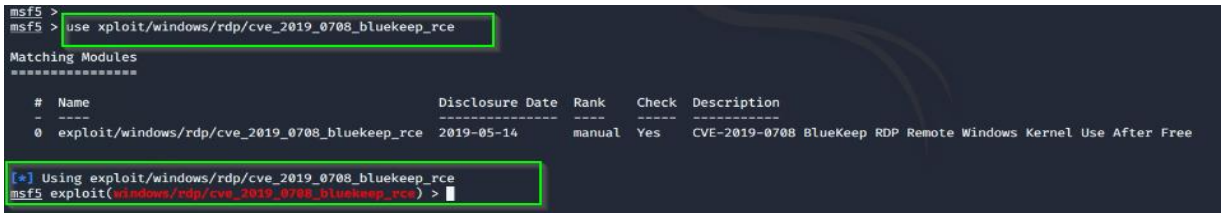


Figura 96. Exploit uso
Fuente: Autores

En la figura anterior se hizo la búsqueda de la vulnerabilidad y se selecciona la utilización para explotación de rdp de Windows y se procede a configurar dicho payload.

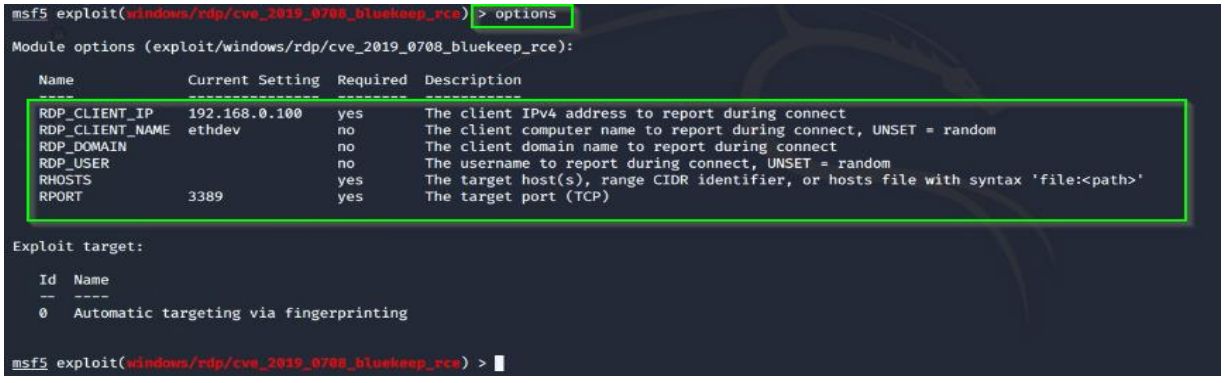


Figura 97. Requerimientos de una explotación
Fuente: Autores

Al ejecutar el comando *options* se muestra los requerimientos necesarios para realizar la explotación.

Figura 98. Configuración de payload
Fuente: Autores

Posteriormente se procede en la figura 98 a configurar el payload con los datos necesarios para la explotación, en color verde la IP de la máquina objetivo siendo la 192.168.41.159, de color rojo la máquina atacante (atacante outsider) con IP 192.168.41.99, y el puerto que queremos explotar que es el puerto RDP de escritorio remoto.

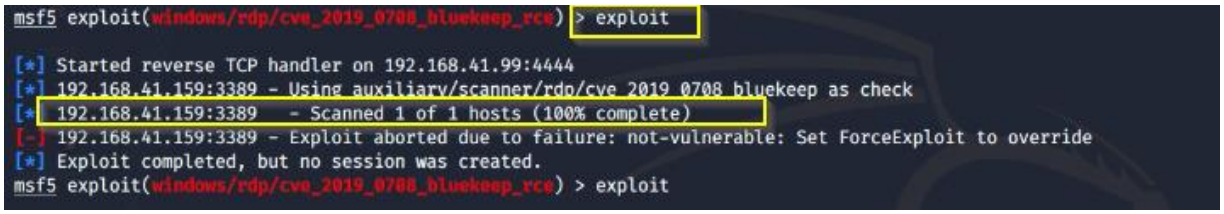


Figura 99. Exploit Ejecución
Fuente: Autores

Una vez configurado el payload con todos sus parámetros se utiliza el comando exploit para ejecutar la explotación del acceso remoto, en donde se señala que se completó en un 100%.

ANEXO 3. FASE DE OPTIMIZACION

En la presente fase los autores plantean aportar a la infraestructura de red agregar una herramienta de criptografía asimétrica, como es Crypto GNUPG, la cual es una herramienta de cifrado y firmas digitales, permitiendo establecer conexiones seguras entre dos partes autenticando mutuamente a dichas partes.

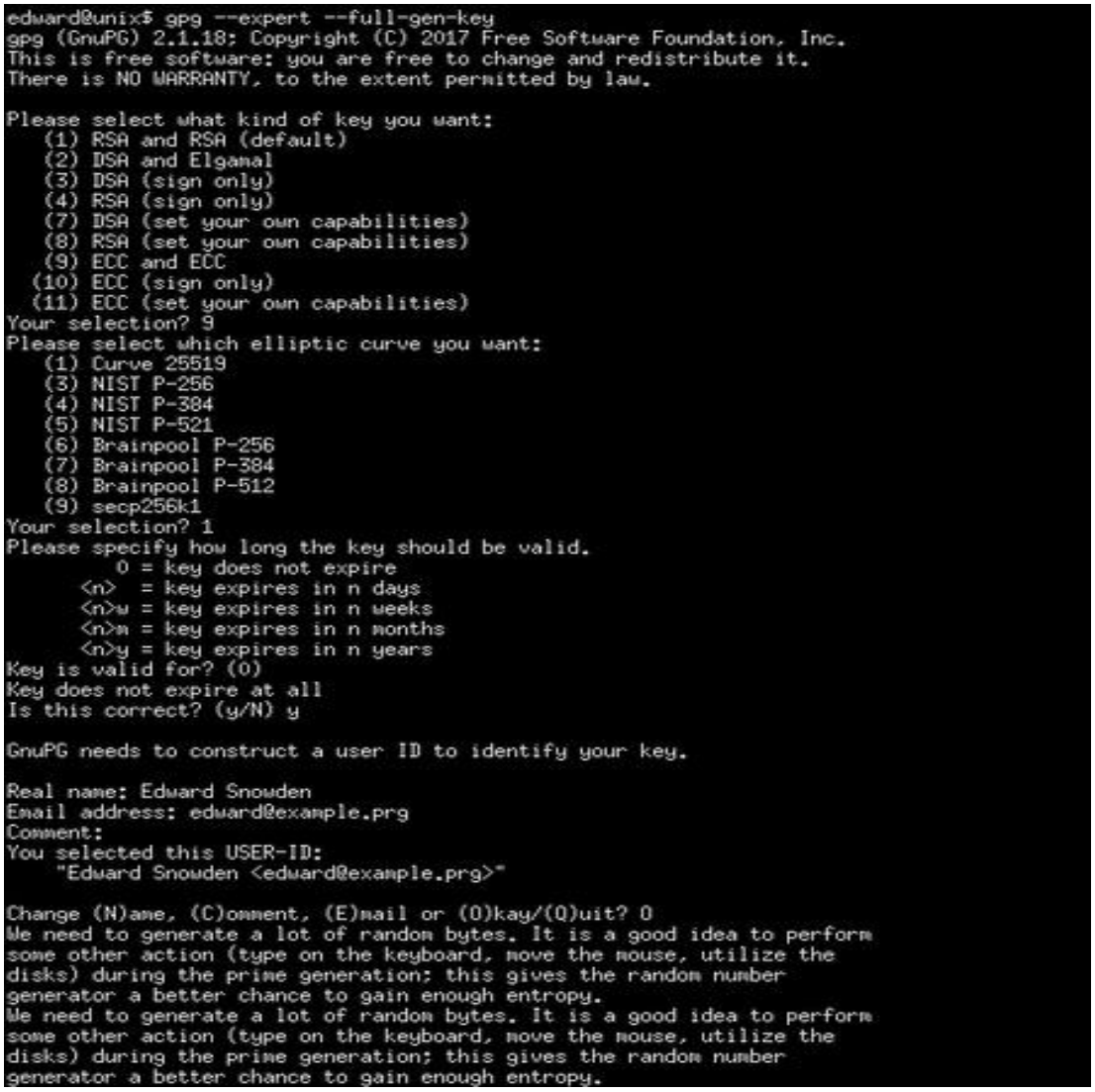


Figura 100. Imagen referencial de la herramienta
Fuente: Wikipedia.org

Figura 101. Imagen referencial de instalación GNUPG y otras herramientas
Fuente: Javier Domínguez Gómez versión 0.03-2017 Guía de instalación GNUPG

ANEXO 4. ENTREVISTA

Hospital de Especialidades Portoviejo

Maestría en Tecnología de la Información Mención Redes y Sistemas Distribuidos

Información de la entrevista

Fecha: _____ Hora: _____

Nombre entrevistado: _____

Cargo: _____

Email: _____

Teléfono: _____

Datos del entrevistador

Nombre: _____

Email: _____

1. ¿Conoce usted que es un sistema de correlación de eventos?

2. ¿Conoce usted el concepto de defensa en profundidad aplicada a TI y a ciberseguridad?

3. ¿Cuenta el centro de datos de la institución con un sistema de ciberseguridad NG-FW, WAF, IPS, IDS, SIEM?

4. ¿Cuenta el centro de datos de la institución con un sistema de administración y gestión ante ataques cibernéticos?

5. ¿Estaría de acuerdo en desplegar una solución basada en seguridad en profundidad con tecnología SIEM?

6. ¿Ha sido víctima de un ataque cibernético?

7. ¿Qué mecanismo aplica ante un ataque cibernético?

Anexo 5 Plan de Mejoras

PLAN DE FORTALECIMIENTO ANTE ATAQUES INFORMÁTICOS DEL HOSPITAL DE ESPECIALIDADES PORTOVIEJO BASADOS EN SISTEMAS DE CORRELACIÓN DE LOG

ESPAMMFL
ESCUELA SUPERIOR POLITÉCNICA
AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

CONTENIDO

CONTENIDO DE CUADROS Y FIGURAS

1. INTRODUCCION

El propósito del plan de fortalecimiento ante ataques informáticos basado en la Correlacion de Logs en la infraestructura del centro de datos del Hospital de Especialidades Portoviejo, que mediante la utilización de la herramienta AlienVault OSSIM siendo este un SIEM y puesto a prueba en un ambiente controlado se describe una solucion tecnología para poder mitigar los posibles ataques e intrusiones no autorizadas dentro de la red e inspeccionar servicios y actividades trascendentales ejecutados en tiempo real, para determinar una serio de mecanismos y estrategias en función de prioridades aplicado dentro del departamento de TI, que pueda afectar tanto el funcionamiento de los dispositivos que conforman la red del hospital, como también al personal del centro de datos, el personal médico y los pacientes.

Así mismo, se logran detectar y detener anomalías dentro de la infraestructura de red, los cuales incitarían en los servicios prestados por la institución, y poder conservar la disponibilidad, seguridad y la confidencialidad en las actividades dentro del HEP.

Davyt (2017) manifiesta que cada vez es evidente que los mecanismos de seguridad se han incrementado de una manera considerable en los servicios de red, desde servidores y otros dispositivos, por lo cual es necesario aplicar estrategias de seguridad, como herramientas necesarias para la detección de virus, y el difícil acceso a la información, la misma que no puede ser identificada por las personas, siendo fundamental disponer de componentes que permitan identificar eventos anómalos o normales que representan un conflicto para la empresa.

2. ALCANCE

Este plan de fortalecimiento ante ataques informáticos es aplicable para el Hospital de Especialidades Portoviejo objeto de nuestra investigación en donde se hizo un estudio de monitoreo para determinar el estado de la red actual y analizar las posibles alternativas de mejoras para robustecer la infraestructura

de red mediante mecanismos de ciberseguridad centralizada el cual se propone la utilización de AlienVault OSSIM de acuerdo al análisis previamente realizado de las herramientas SIEM que cumplan con el requisito de software libre.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Elaborar un plan de fortalecimiento ante ataques informáticos basado en correlación de logs.

3.2 OBJETIVOS ESPECIFICOS

- Definir la herramienta SIEM a utilizar
- Ejecutar análisis de vulnerabilidades y ataques controlados dentro de la nueva infraestructura de red propuesta
- Proponer acciones de mejoras mediante el análisis de los resultados del despliegue del sistema de correlación y flujo de tráfico obtenidos del monitoreo de la red.

4. ENFOQUE

El plan va enfocado a la implementación y despliegue de un servidor de correlación de eventos de log dentro del centro de datos del HEP, tomando como referencia la topología de red del centro de datos actual y proponiendo una nueva solución, incorporando el SIEM en un punto estratégico de la red de datos del DMZ, como mecanismo de seguridad centralizada y defensa en profundidad, y que a través de los resultados obtenidos se hace un análisis comparativo del antes y el después, emitiendo recomendación.

La institución cuenta con un ancho de banda de 50 MB, suministrada por CNT, y un enlace secundario backup suministrada por Alfanet con un ancho de banda de 50 MB haciendo un balanceo de carga multiwan definiendo de manera automática los tier 1 y tier 2.

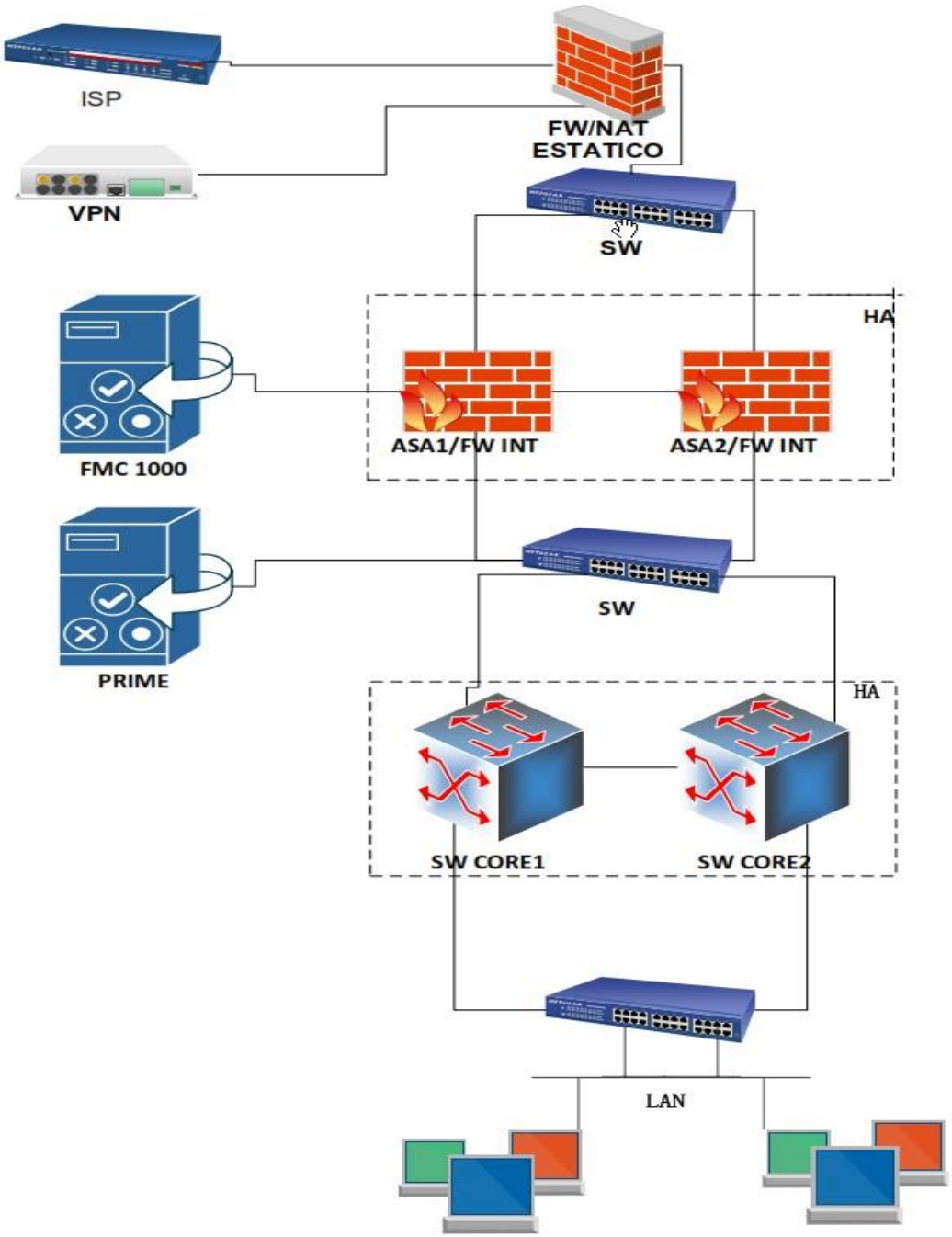


Figura 102. Diagrama de Red Hospital de Especialidades
Fuente: Autores

Según el diagrama de red actual del Hospital de Especialidades Portoviejo, el mismo es un modelo de red de núcleo colapsado, en el cual se tienen varias capas para la interconexión y comunicación de los dispositivos de red, pero existe una gran deficiencia en cuanto al control y seguridad de la red, pues muchos de sus sistemas aunque sean robustos en su accionar existe la falencia

del licenciamiento para poder funcionar al 100% o poder explotar totalmente sus características tecnológicas.

Además de lo mencionado tanto el FW como los IDS, y los dispositivos de red generan logs los mismo que son tratados independientemente por cada equipo, en ciertos casos incluso dichos logs no son tomados en cuenta y no existe un tratamiento de dicha información, provocando un desconocimiento en el personal de TICs del Hospital de Especialidades Portoviejo en cuanto a la existencia o no de posibles ciberataques en tiempo real, así como no contar con una herramienta cuadro de mando que permita tomar decisiones o realizar políticas de mejoras en ciberdefensa.

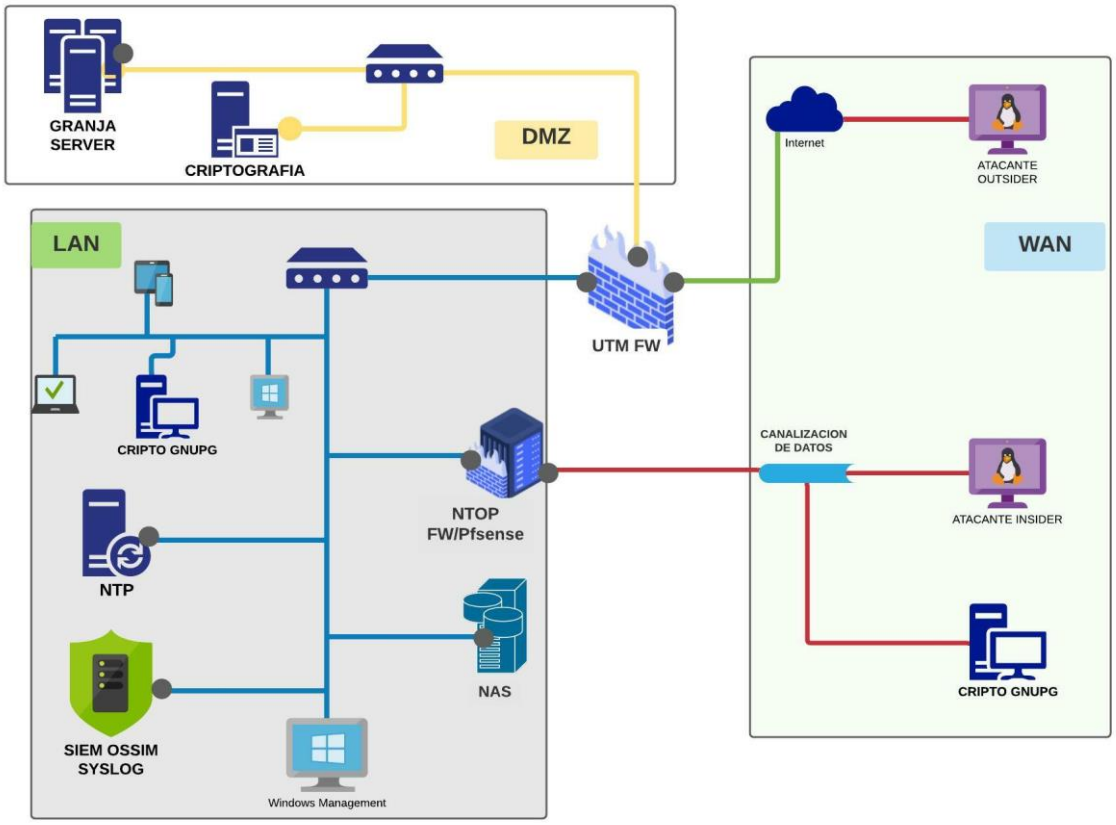


Figura 103. Diagrama de laboratorios propuesto
Fuente: Autores

En el diagrama propuesto para esta investigación se presenta un nuevo esquema de red, en la que todos los elementos que intervienen trabajen de manera síncrona, permitiendo colectar los eventos que ocurren en la red del HEP, la cual está basada en un sistema de correlación de eventos, de esta manera los diferentes eventos pueden ser tratados y permitir a los sistemas de

monitorización analizar los paquetes entrantes y salientes, toda esta información será analizada con la herramienta OSSIM, lo cual permitirá tener una defensa en profundidad con la cual se pretende aplicar controles de seguridad para proteger los datos en diferentes capas.

5. GLOSARIO DE TERMINOS

CÓDIGO ABIERTO	Se refiere a cualquier programa cuyo código fuente se pone a disposición para su uso o modificación, conforme los usuarios u otros desarrolladores lo consideren conveniente (TechTarget, 2021)
CONTROL	Es el mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos en dominio, mando y preponderancia, o a la regulación sobre un sistema
DISPONIBILIDAD	Es el acceso de personas u organismos a diversos datos, mediante mecanismos seguros y sencillos, que garanticen los procesos que información de una empresa (IBM, 2015)
ESTRATEGIA DE MONITOREO	Según el autor es una propuesta que indica una serie de acciones de mejoras que conlleva a la mitigación de problemas defectuosos o lentos en el control de la red para dar solución a nivel empresarial.
EVENTOS	Es un proceso que se enfoca a la gestión de la seguridad que busca proporcionar una visión de seguridad de la tecnología de la información (TI) de una organización (Rouse, 2019)
HERRAMIENTAS DE MONITOREO	Son sistemas de diagnóstico para telecomunicaciones, servidores o redes que buscan componentes defectuosos o lentos, con el fin de informar a los administradores mediante correo electrónico, sms, entre otros (Nagios, 2016).

RED DE DATOS	Un conjunto de equipos y dispositivos que están conectados entre sí, y comparten recursos, información, y servicios (VIU, 2020).
DATA CENTER	Centro de proceso de datos es una ubicación que concentra todos los recursos físicos para el procesamiento de la información de una empresa u organización
SNORT	Sistema de detección de intrusos con licencia GNU, ofrece la capacidad de almacenamiento de bitácoras en archivos de texto y en bases de datos abiertas (Snort, n.d.), Ossim tiene una versión personalizada la cual nos da las alertas sobre los intrusos a nuestra red.
OPENVAS	Es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas no autenticadas, pruebas autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un poderoso lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad(OpenVas, n.d.).
NTOP	Es una herramienta Open Source para la monitorización del tráfico de la red en tiempo real, permite controlar el consumo de recursos por parte de los usuarios y aplicaciones que se usen a diario y detectar más las configuraciones de equipos(NTOP, n.d.).
NAGIOS	Es un sistema de monitorización de redes ampliamente utilizado que nace en 1999, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado” (Nagios, 2021)

NMAP	Es un escáner de red, que permite crear inventarios de los sistemas o host activos en la red, en otras palabras es una herramienta para la exploración de redes, permite escanear los puertos de las máquinas que se encuentra en la red, se puede identificar si un puerto está abierto, cerrado o se encuentra protegido, determina que servicios se encuentran utilizados por los equipos de la organización, incluso muestra la información del sistema operativo. (Robiedo , 2011).
OPEN SOURCE	Expresión con la que se conoce al software distribuido y desarrollado libremente.
OSSIM	Open Source Security Information Management por sus siglas es una colección de herramientas bajo la licencia GPL, diseñadas para ayudar a los administradores de red en la seguridad de las computadoras, detección de intrusos y prevención (Bravo et al., 2015).
SEM	Gestión de Eventos, proporciona monitoreo en tiempo real y gestión de eventos de TI de apoyo a las operaciones de seguridad(Agrawal & Makwana, 2013).
SIM	Gestión de la Seguridad de la Información, permite tener una historia de los sucesos. Monitor: Realiza una monitorización de la red ayudando al administrador de seguridad a reconocer si un evento está presentando alguna actividad anómala(Agrawal & Makwana, 2013).
SENSOR	Recoge los logs de los diferentes dispositivos electrónicos y aplicaciones de seguridad.
AlienVault	Es un sistema unificado de gestión de seguridad, el cual integra una serie de herramientas para la seguridad informática.(Bowling, 2010)

CLOUD COMPUTING	La computación en la nube, concepto conocido también bajo los términos servicios es un paradigma que permite ofrecer servicios de computación a través de Internet (RedHat, 2018).
DNS	Abreviatura para Sistema de nombre de dominios, que permite asignar nombres a equipos y servicios de red(Fernadez, 2018).
NAS	Network-Attached Storage, es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento (Fernadez, 2018).
KERNEL	Software que constituye una parte fundamental del sistema operativo(Fernadez, 2018).
VIRTUALIZACIÓN	Es la creación a través de software de una versión virtual de algún recurso tecnológico(Fernadez, 2018).
ROOT	Usuario genérico en Linux que tiene acceso administrativo al sistema(Fernadez, 2018).
HTTP	Protocolo de transferencia de hipertextos, que se utiliza en algunas direcciones de internet.
SMTP	Protocolo de la capa de aplicación. Protocolo de red basado en texto, utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (IONOS, 2018)
ICMP	Protocolo de Mensajes de Control de Internet o ICMP es el sub protocolo de control y notificación de errores del Protocolo de Internet (Lopez, 2021).
SSH	Sirve para acceder a máquinas remotas a través de una red.
IAAS	La infraestructura como servicio proporciona a las empresas recursos informáticos, incluyendo servidores, redes, almacenamiento y espacio en centro de datos con pago en función del uso (IBM, 2021).

PAAS	Plataforma como servicio proporciona un entorno basado en cloud con todos los requisitos necesarios para dar soporte a todo el ciclo de vida de creación y puesta en marcha de aplicaciones basadas en web (cloud) (IBM, 2021)

6. GESTION DE EVENTOS DE SEGURIDAD Y SU APLICABILIDAD EN LA INFRAESTRUCTURA DE RED DEL HEP

La dependencia de contar con una infraestructura computacional en las instituciones públicas o privadas conlleva un intrínseco control sobre dicha infraestructura, en el trabajo de (Quintero & Tovar, 2019), se define como sistema de monitorización y gestión de eventos de seguridad al conjunto de sistemas, normativas y protocolos de gestión que facilitan las actividades de detección y prevención ante anomalías dentro la infraestructura tecnológica.

Con referencia de lo enunciado, esta estrategia es ajustable a la institución objeto de estudio, dado que usa cantidad de datos y registros, es imperante el uso de controles para impedir posibles ataques informáticos y mantener los servicios activos de forma constante en la institución. Por lo demás, el sistema propuesto para llevar la gestión de la seguridad informática y hacer posible la optimización de la infraestructura actual.

7. ELEMENTOS DE EJECUCION DEL AMBIENTE CONTROLADO

Como herramienta base para la implementación del laboratorio se procede con la instalación de sistemas de virtualización, dentro de la misma se procederá con la instalación y configuración de las siguientes máquinas virtuales y físicas para lograr los objetivos de la presente investigación, cabe mencionar que todos

los sistemas operativos y herramientas utilizadas en la presenten investigación son de carácter de libre distribución:

Tabla 16. Máquinas Virtuales y Herramientas Utilizadas

MAQUINAS VIRTUAL	HERRAMIENTAS
Kali Linux	NMAP
Windows Server	Metasploit Framework
Windows cliente (Windows 7)	Openvas
Firewall IPCOP	Nagios
Firewall PFSENSE	La Hidra
Firewall MONOWALL	
FREENAS	
AlienVault OSSIM	

Fuente: Autores

8. SELECCIÓN Y CATEGORIZACIÓN DE HERRAMIENTAS PARA MONITOREO

En la tabla a continuación se describen las soluciones SIEM, identificando cada una de ellas si cumplen los criterios de software libre propuesto para el desarrollo de esta investigación.

Tabla 17 Comparativa herramientas Siem.

Herramienta	Fuente	Observaciones	Aplica/No aplica
IBM QRADAR	https://www.ibm.com/es-es/products/qradar-siem	Herramienta de software propietario	No

HP ArcSight	https://www.microfocus.com/es-es/products/siem-security-information-event-management/overview	Herramienta de software propietario	No
Splunk	https://www.splunk.com/en_us/software.html	Herramienta con licencia GNU	Si
SolarWinds	https://www.solarwinds.com/security-event-manager	Herramienta de software propietario	No
AlienVault	https://cybersecurity.att.com/products/ossim	Herramienta que cuenta con la solución OSSIM (open source) con licencia GNU	Si
Mozdef	https://mozdef.readthedocs.io/en/latest/overview.html	Herramienta con licencia GNU	Si
EventTracker	https://www.netsurion.com/managed-threat-protection	Herramienta de software propietario	No

Fuente: Autores

En la siguiente tabla haremos una comparativa de las herramientas que si aplica a Open Source, identificando sus características significativas.

Tabla 18 Comparativas de productos Open Source Siem

Herramienta ***Descripción***	**Splunk**	**AlienVault OSSIM**	**Mozdef**
Basado en GNU	✓	✓	✓
Capacidad de almacenamiento y procesamiento de logs.	Limitada	Limitada	**X**
Transferencia segura de datos	✓	✓	✓

Visualizaciones de estados continuo	✓	✓	✓
Normalizador de Eventos	✓	✓	✓
Balanceo de carga/clúster	✓	✓	✓
Interfaz personalizables	✓	✓	✓
Años de experiencia	15 años	12 años	10 años
Sito web	✓	✓	✓

Fuente: Autores

De acuerdo al análisis y comparativas realizadas tanto de las herramientas Open Source como las de software propietario, se toma en consideración la utilización para esta investigación la solución AlienVault Ossim, la cual incluye varios componentes usables para el correcto funcionamiento del proyecto y por destacarse en sus calificaciones de prestaciones.

8.1 OSSIM ALIEN VAULT

AlienVault OSSIM (Open Source Security Information Manager) una solución Siem, fue desarrolla en el año 2000, la cual incluye las técnicas de prevención y detección de intrusos en la seguridad general de una red, también funciona a raíz de un conjunto de herramientas de monitoreo y seguridad con licencia GNU (Open Source), tales como Nagios, Snort, Openvas, Ntop, entre otras. Por lo tanto ofrece una gran capacidad y rendimiento en sus análisis, gestión, organización de los eventos que se producen entorno a la red en función, dado que la mayorías de sistemas Siem no dan estas prestaciones, siendo una herramienta factible para su uso por muchos factores ya mencionado (Bowling, 2010).

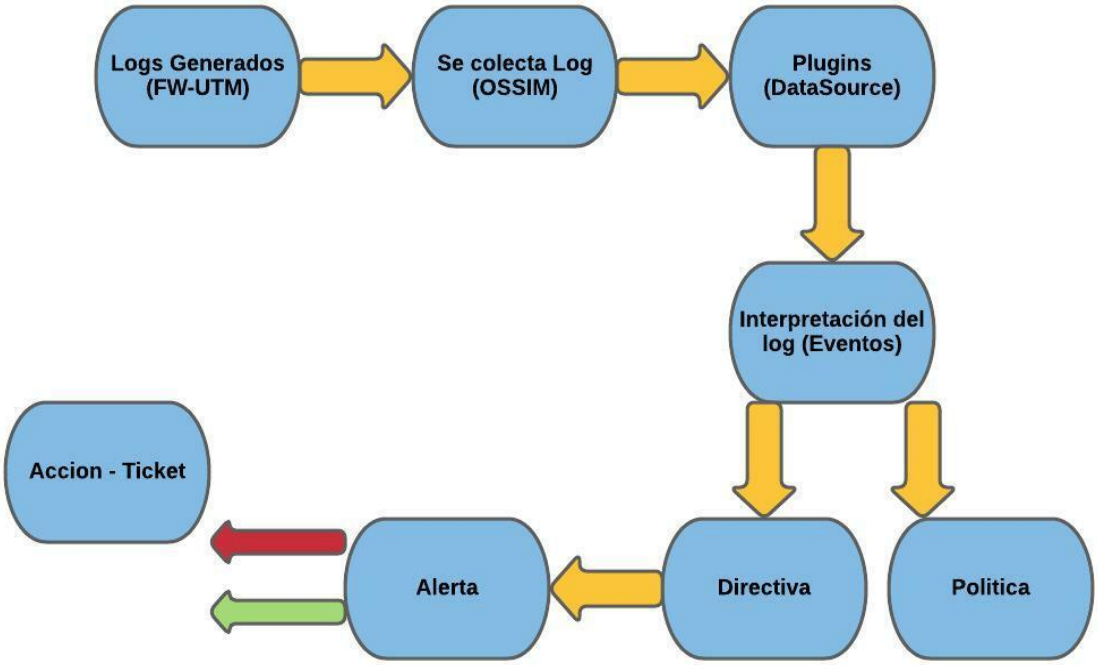


Figura 104 Concepto Correlacion de Logs
Fuente: Autores

La correlación de eventos se realiza generalmente para obtener un conocimiento de la información de más alto nivel que nos puede proporcionar los eventos, por ejemplo, identificar situaciones extraordinarias, para identificar la causa raíz de un problema, o para realizar predicciones sobre el futuro y descubrir tendencias.

Existen diversos enfoques para la que puede ser útil la correlación de eventos, como análisis de datos de mercado, detección de fraude (por ejemplo, detectar los patrones de uso infrecuente de una tarjeta de crédito), análisis de logs del sistema (por ejemplo, agrupar mensajes similares y aumento de acontecimientos importantes) o análisis de gestión y fallas de red (por ejemplo, detectar la causa de un problema de red)(Müller, 2009)

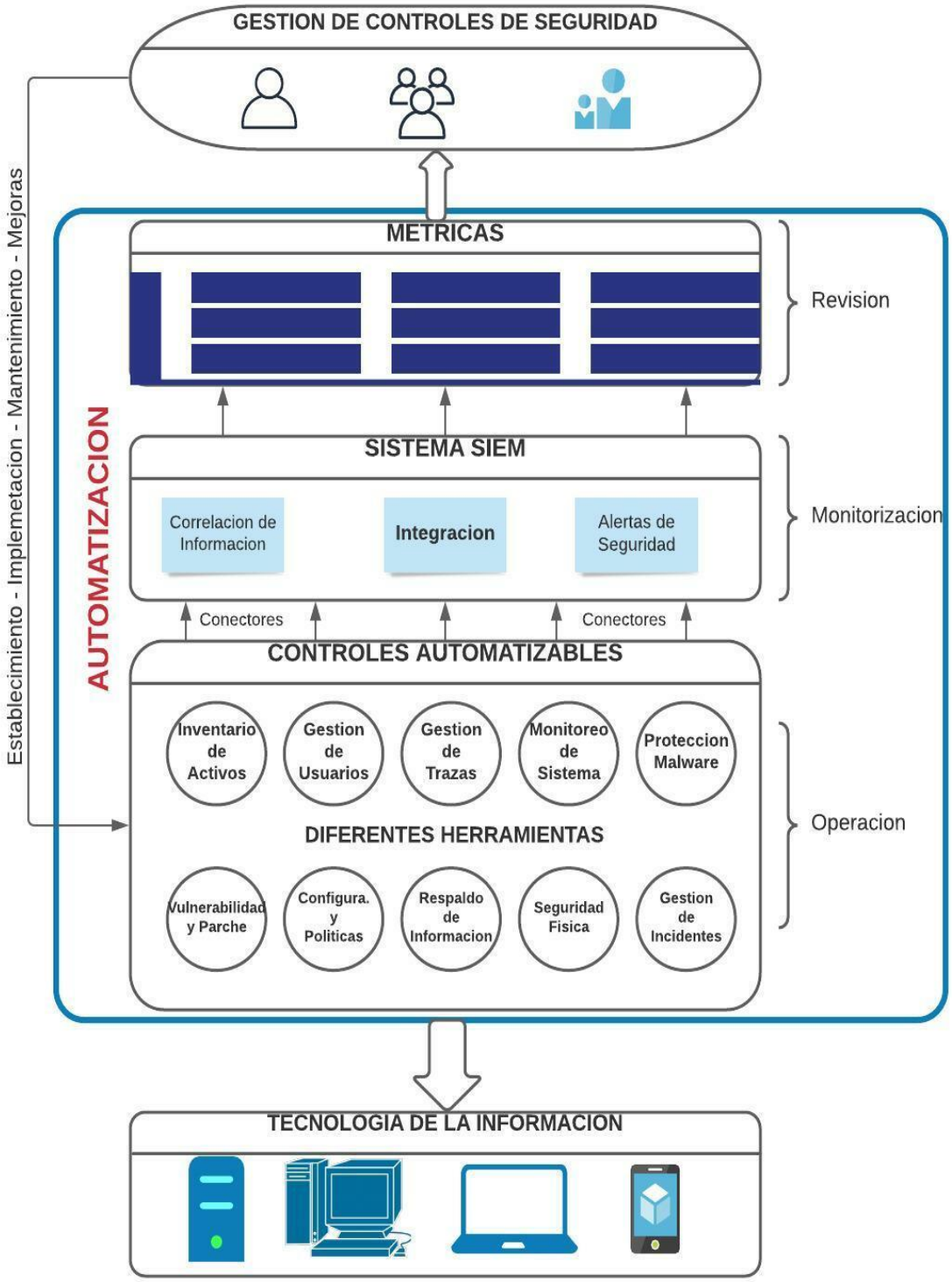


Figura 105 Modelo para la gestión automatizada e integrada de controles de seguridad
Fuente: (Montesin, Garcia, & Rubier, 2013)

El modelo de gestión automatizada e integrada de controles de seguridad posee las siguientes características generales: revisión, monitorización y

operación, dentro de los cuales se encuentran inmersos las métricas, sistema Siem, y controles automatizables.

Revisión: De acuerdo a la definición de automatización de controles de seguridad informática presentada en este trabajo, es posible automatizar también la revisión de los controles de seguridad informática. Para lograr este propósito es necesario definir un grupo de indicadores y métricas que permitan evaluar continuamente la efectividad de los controles(Montesino et al., 2013).

Monitorización: El sistema SIEM es el componente central del modelo, permitiendo la integración de diferentes herramientas de seguridad informática, el seguimiento centralizado de los controles, la correlación de información y la generación de reportes de seguridad de forma automatizada(Montesino et al., 2013).

Operación: Los controles de seguridad informática son implementados y operados por diferentes sistemas, pero su monitorización se realiza de forma centralizada en el sistema SIEM(Montesino et al., 2013).

El modelo propuesto constituye un marco de trabajo, a raíz de la anexión de actividades de estudio de controles por medio de un conjunto de reglas determinadas en la investigación, se describen los mecanismos y acciones que se pueden automatizar en la implementación y despliegue de una estrategia de defensa en profundidad basada en un sistema de correlación de eventos SIEM.

9. PROCESOS Y PROCEDIMIENTOS

A continuación se da a conocer los procesos y procedimientos aplicados en el plan de mejoras antes ataques informáticos en el Hospital de Especialidades Portoviejo.

Tabla 19 Descripción de los procesos y procedimientos

PROCESOS	PROCEDIMIENTOS
Análisis de requerimiento	Se identifica los procesos que conlleva la infraestructura de red entre ellos: • Almacenamiento • Plataforma IAAS • Servicios (Base Datos, Correos, FW, IDS, IPS, Herramienta de monitorización, Seguridad, Sistema de correlación) • Seguridad Centralizada (Hardenización, criptografías, esteganografía, herramientas de correlación anómalos WAF)
Planteamiento de estrategias de gestión de seguridad centralizada	Estrategias y mecanismos de gestión para determinar la topología de la infraestructura tecnológica.

	Se escoge la herramienta de gestión para la seguridad
Determinación e implementación de herramientas para el monitoreo de redes de computadoras	Se implementan las herramientas en el plan de mejoras ante ataques informáticos entre las cuales tenemos: • IPCOP/NTP • MONOWAL • PFSENSE • FREENAS • OSSIM
	Reportes de la infraestructura tecnológica.
	Reportes de ataques detectados por la herramienta de gestión en tiempo real.
Análisis de monitoreo	Se implementan los mecanismos de gestión y control para proteger la información y tener un mejor rendimiento en la infraestructura tecnológica.
Acciones de mejora	Mecanismos y reglas de control dentro de la red tecnológica y así poder detener anomalías en los eventos registrados por los diversos dispositivos.

Fuente: Autore

10. ANÁLISIS DE VULNERABILIDADES Y ATAQUES DENTRO DE LA NUEVA INFRAESTRUCTURA DE RED PROPUESTA.

En las figuras 1 vemos un análisis de vulnerabilidad realizado por la herramienta SIEM, permitiendo obtener la cantidad de vulnerabilidades encontradas en dichos nodos,

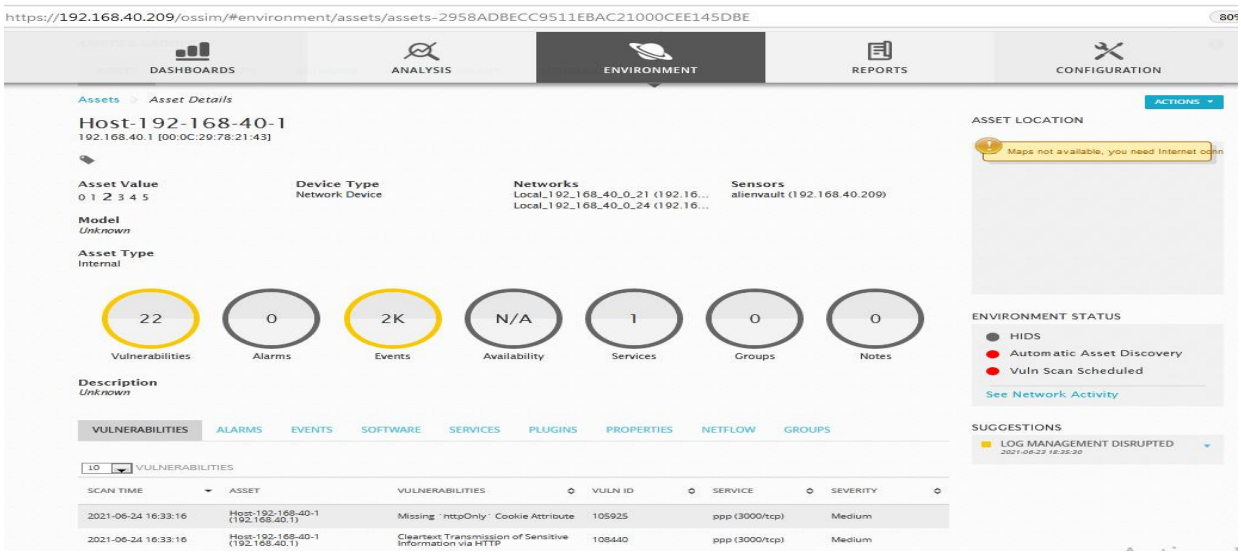


Figura 106 Análisis Vulnerabilidades
Fuente: Autores

10 VULNERABILITIES

SCAN TIME	ASSET	VULNERABILITIES	VULN ID	SERVICE	SEVERITY
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	Missing `httpOnly` Cookie Attribute	105925	ppp (3000/tcp)	Medium
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	Cleartext Transmission of Sensitive Information via HTTP	108440	ppp (3000/tcp)	Medium
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	Cleartext Transmission of Sensitive Information via HTTP	108440	http (80/tcp)	Medium
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	CGI Scanning Consolidation	111038	ppp (3000/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	CGI Scanning Consolidation	111038	http (80/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	jQuery Detection	141622	http (80/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	nginx Detection	100274	http (80/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	ntopng Version Detection	107109	ppp (3000/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	OS Detection Consolidation and Reporting	105937	general (0/tcp)	Info
2021-06-24 16:33:16	Host-192-168-40-1 (192.168.40.1)	pfSense Detection (Version)	112118	general (0/tcp)	Info

Figura 107 Descripción de Vulnerabilidades

Fuente: Autores

En la figura 3 y 4 observamos el número y nivel de severidad de las vulnerabilidades, el equipo afectado corresponde al Pfsense con la IP 192.168.40.1, y la descripción de las vulnerabilidades entre las que tenemos nginx Detection, JQuery Detection entre otros.

Podemos ver en las siguientes figuras un ataque de fuerza bruta registrado por el SIEM y la herramienta NIDS (Sistema de Detección de Intrusos de Red), que nos registra también desde donde se originó el ataque (IP origen 192.168.40.123) y cuál fue su destino (IP destino 192.168.40.81), señalando el puerto utilizado, a su vez en las figuras 4 y 5 nos refleja que el password no está encriptado y las reglas de detección del ataque.

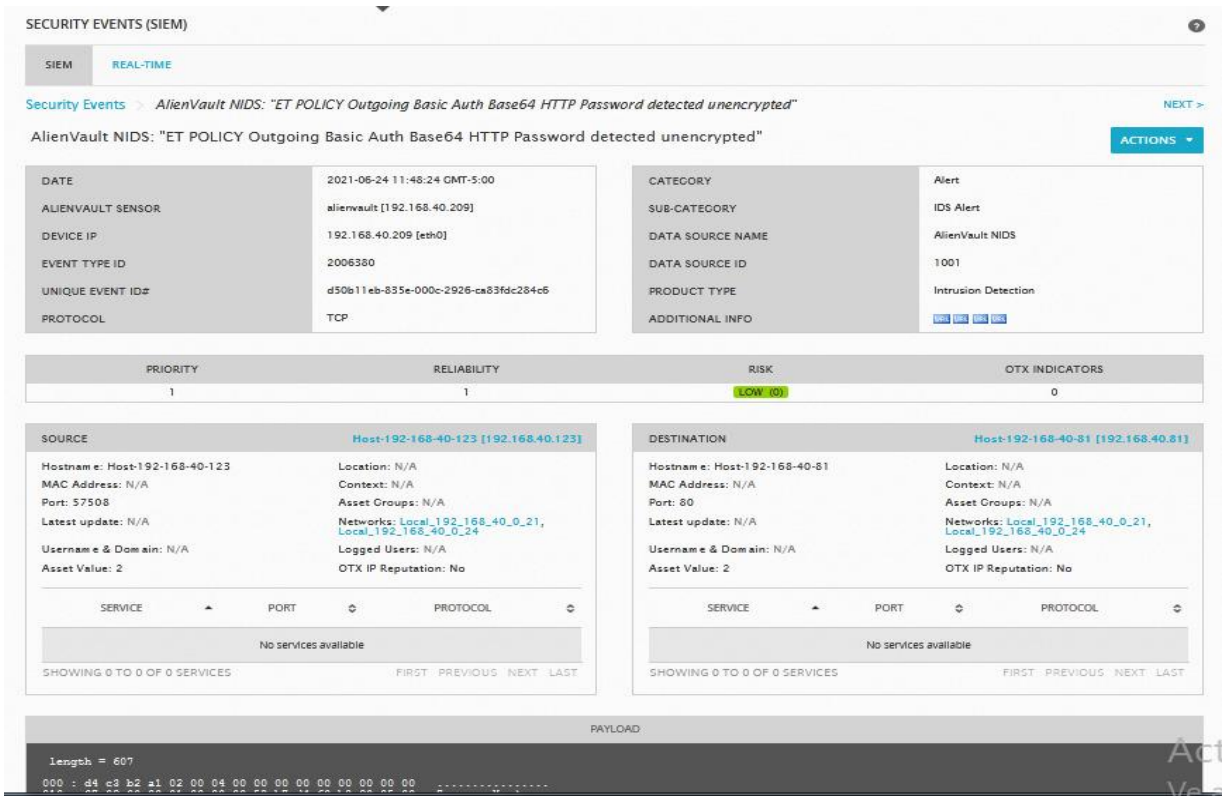


Figura 108. Ataque Detectado
Fuente. Autores

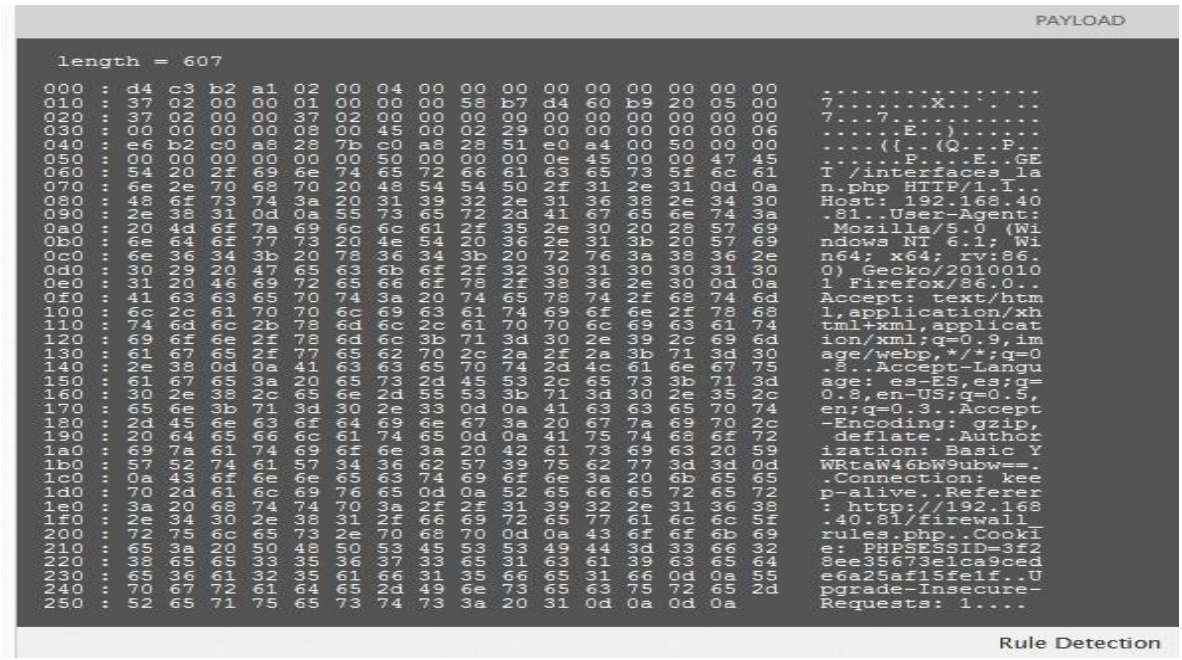


Figura 109. Descripción del ataque
Fuente: Autores

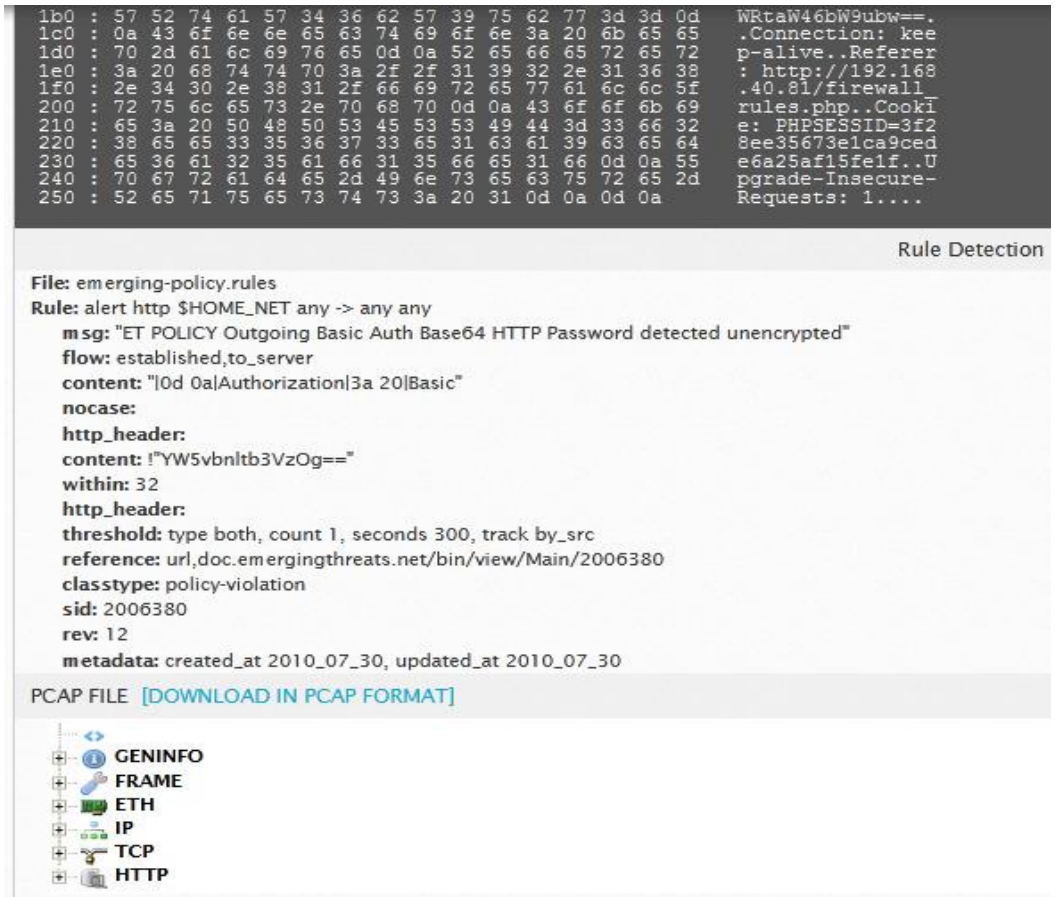


Figura 110. Descripción ataque
Fuente: Autores

11. ACCIONES DE MEJORAS MEDIANTE EL ANÁLISIS DE LOS RESULTADOS OBTENIDOS DEL MONITOREO DE LA RED.

Las acciones de mejoras en los resultados obtenidos de verán reflejados de la siguiente manera.

- Rango de uso
- Rango de ejecución.
- Indicadores de estados
- Complejidad de la herramienta.
- Generación de ticket, alertas y notificaciones por medio de email.
- Revisión de monitoreo activo
- Ejecución de técnicas y mecanismos
- Efectuar mantenimientos correctivos y preventivos.
- Dar solucion de mejora en la infraestructura tecnológica.

12. ESTRATEGIA DE MONITOREO Y GESTION DE SEGURIDAD.

Para realizar estrategias de monitoreo y gestión de seguridad centralizada tenemos las que podemos nombrar:

- Contar de un ancho de banda.
- Gestión de uso de memoria.
- Conexiones físicas en buen estado.
- Afluencia de tráfico.
- Alarmas para garantizar el buen funcionamiento de los dispositivos de red.
- Ejecutar acciones de monitoreo.
- Selección de sistemas y equipos a usar en la topología de red.
- Estadísticas de uso de la red tecnológica.

- Mantener la función de disponibilidad 24/7 en la infraestructura.
- Realizar priorización en los procesos de monitoreo.
- Análisis de los eventos en la herramienta en tiempo real.
- Ejecutar mejoras para dar soluciones a posibles anomalías dentro de la red.

Tabla 20. REGLA DE FW PARA EQUIPO UTMFW

REGLAS EN EL FIREWALL EN LA INTERFAZ LAN								
State	**Protocol**	**Source**	**Port**	**Destination**	**Port**	**Gateway**	**Queue**	**Description**
0/0B	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none	Regla DNS
0/0B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none	Regla HTTP NAVEGACON
0/0B	IPv4 TCP	LAN net	*	*	81 (HTTP)	*	none	Regla HTTP NAVEGACON port 81
0/0B	IPv4 TCP	LAN net	*	*	8080 (HTTP)	*	none	Regla HTTP NAVEGACON port 8080
0/0B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none	Regla HTTPS NAVEGACON SEGURA
0/0B	IPv4 TCP	LAN net	*	*	22 (SSH)	*	none	Regla SSH
REGLA PARA HABILITAR EL PUERTO RDP 3389 DEL SYS ADMIN								
State	**Protocol**	**Source**	**Port**	**Destination**	**Port**	**Gateway**	**Queue**	**Description**

0/0B	IPv4 TCP	Single host or alias 192.168.40.123	*	*	3389 (RDP)	*	none	Regla RDP SYS ADMIN 3389

CREACION DE REGLAS DESDE LA LAN HACIA EL DMZ

State	Protocol	Source	Port	Destination	Port	Gateway	Queue	Description
0/0B	IPv4 TCP	LAN net	*	OPT1 net	1898 (other)	*	none	Regla LAN a DMZ HTTP 1898 Lampiao
0/0B	IPv4 TCP	LAN net	*	OPT1 net	5900 (vnc)	*	none	Regla LAN a DMZ SERVER VNC 5900
0/0B	IPv4 TCP	LAN net	*	OPT1 net	445 (SMB)	*	none	Regla LAN a DMZ SERVER SMB 445

HABILITAR REGLAS DE PORT FORWARD EN LA WAN

Interface	Protocol	Source Address	Source port	Dest Address	Dest Port	NAT IP	NAT Ports	Description
WAN	TCP	*	*	WAN Address	1898	192.168.8.130	1898	DNAT Port forward 1898 Lampiao server http
WAN	TCP	*	*	WAN Address	HTTP (80)	192.168.8.128	HTTP (80)	DNAT Port forward PUERTO 80 http Metasploit
WAN	TCP	*	*	WAN Address	3389	192.168.40.123	3389	DNAT Port forward RDP 3389 Windows 7

WAN	TCP	*	*	WAN Address	8001	192.168.41.159	8080	DNAT	Port forward SERVER HTTP BADBLUE REGLA

Fuente: Autores

Tabla 21. Políticas de amenazas Ossim

POLÍTICAS DESPLEGADAS HERRAMIENTA OSSIM									
CONDICIONES					CONSECUENCIAS				
Origen	**Destino**	**Src. Port**	**Dst. Port**	**Tipo evento**	**Accion**	**SIEM**	**Logger**	**Reenvío eventos**	**Descripción**
ip, red, grupos de red, any	ip, red, grupos de red, any	ssh	ssh	any	full ssh sin password	SIEM: si	no	no	Política para evitar falsos positivos SSH
						Prioridad evento: no cambio			
						Riesgo: si			
						Correlación logica: si			
						Correlación cruzada: si			
						almacenamiento SQL: si			
		www	www	any	no action	SIEM: si	yes	no	

ip, red, grupos de red, any	ip, red, grupos de red, any	Prioridad evento: no cambio Riesgo: si Correlación lógica: si Correlación cruzada: si almacenamiento SQL: si	Política para monitorear tráfico www

Fuente: Autores

13. APROBACIÓN Y APLICACIÓN

En la ejecución de esta etapa, se consideran que los sistemas de gestión y monitoreo de una estrategia de defensa en profundidad basados en sistemas de correlación de eventos implementados sean óptimos y que ejecuten sus métodos eficaz y efectivamente en el control de monitorización, detección y prevención de ataques informáticos dentro de la red tecnológica, de manera que se adapten en la infraestructura de red y permitan arrojar datos relevantes del análisis de monitoreo y gestión centralizada, y así apoyar en las funciones de gestión y rendimiento que se lleven a cabo en los procesos de la institución, de manera que si existan problemas se puedan conocer y efectuar soluciones de mitigación en tiempo real, proponer mejoras proactivas y mantener una correcta toma de decisiones.

14. CONCLUSIONES Y RECOMENDACIONES

14.1 CONCLUSIONES

- La implementación de la herramienta de gestión y monitoreo de seguridad centralizada basada en correlación de logs permite optimizar los recursos de la red con la que cuenta el Hospital de Especialidades Portoviejo. La topología propuesta en la investigación admite la distribución de la seguridad de manera más eficaz.

- Se realizaron análisis de vulnerabilidades y ataques dentro de la nueva infraestructura de red propuesta en ambiente controlado y en ambiente de producción basados en la metodología OSSTMM, tenemo: Escaneo de Puertos, inyección SQL, Denegación de Servicio, Payload y Fuerza Bruta, por los cuales se comprobó la validez en la detección de eventos de seguridad informática gestionados mediante la herramienta de correlación de logs OSSIM.

- La herramienta AlienVault OSSIM de acuerdo a sus características de requerimiento de sistema, seguridad, soporte, facilidad de uso y administración es la más recomendable para la implementación.

14.2 RECOMENDACIONES

- Se recomienda la actualización y Hardenización de los dispositivos de defensa perimetral con que cuenta la institución, haciendo posible un mejor control de los posibles ataques generado, así como la posibilidad de la implementación de una estrategia de defensa en profundidad basada en un sistema de correlación de eventos SIEM.

- Se recomienda la utilización de la herramienta de correlación y gestión de eventos AlienVault, debido al hecho de ser de distribución GNU y bajo coste, el cual permitirá mejorar la seguridad en tiempo real del centro de datos del Hospital de Especialidades Portoviejo.

- Se recomienda que al realizar la implementación de un sistema de correlación de eventos, las configuraciones de las políticas que se generen estén configuradas adecuadamente y siempre actualizadas de pendiendo de las reglas o políticas de seguridad de la institución, aunque Ossim tiene una serie de políticas preconfiguradas, es necesario que el administrador configure las políticas acorde al entorno que presenta la organización.

BIBLIOGRAFIA

Agrawal, K., & Makwana, H. (2013). A Study on Critical Capabilities for Security Information and Event Management. In *International Journal of Science and Research* (Vol. 4). Retrieved from www.ijsr.net

Alvino, C. (2021, May 5). Estadísticas de la situación digital de Ecuador en el 2020-2021 | Branch. Retrieved August 26, 2021, from https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-ecuador-en-el-2020-2021/

Ambit. (2019, May 20). La estrategia de seguridad en las bases de datos. Retrieved September 22, 2021, from https://www.ambit-bst.com/blog/la-estrategia-de-seguridad-en-las-bases-de-datos

Ariu, D., Frumento, E., & Fumera, G. (2017). Social Engineering 2.0: A Foundational Work: Invited Paper. *Semantic Scholar*, 319–325. https://doi.org/10.1145/3075564.3076260

Avast. (2021, May 19). ¿Qué es un Cross-Site Scripting (XSS)? | Cómo sucede | Avast. Retrieved September 9, 2021, from Avast Academy website: https://www.avast.com/es-es/c-xss

Bowling, J. (2010). *AlienVault: the Future of Security Information Management* | *Linux Journal*. Retrieved from https://www.linuxjournal.com/article/10649?page=0%2C0

Bravo, H., Villafuerte, L., & Patiño, J. (2015). *Implantación De Una Herramienta Ossim Para El Monitoreo Y Gestión De La Seguridad De La Red Y Plataformas Windows Y Linux Aplicado A Empresas Medianas*. Retrieved from http://www.dspace.espol.edu.ec/handle/123456789/29939

CEH. (2020). Certified Ethical Hacker | CEH Certification | CEH v11 | EC-Council. Retrieved September 8, 2021, from https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

Cordova, J., Vega, H., Rodriguez, C., & Escobedo, F. (2020). FIRMA DIGITAL BASADA EN CRIPTOGRAFÍA ASIMÉTRICA PARA GENERACIÓN DE HISTORIAL CLÍNICO. *3c Tecnologias*, *9*(2254 – 4143), 65–85. Retrieved from https://scholar.google.com/citations?view_op=view_citation&hl=es&user=VhTwpWwAAAAJ&citation_for_view=VhTwpWwAAAAJ:qjMakFHDy7sC

Cornaglia, S., & Vercelli, A. H. (2017). La ciberdefensa y su regulación legal en Argentina (2006-2015)/ The ciberdefense and its legal regulation in Argentina (2006-2015). *URVIO - Revista Latinoamericana de Estudios de Seguridad*, (20), 49–62. https://doi.org/10.17141/urvio.20.2017.2601

Davyt, M. (2017). SIEM: Hacia una nueva estrategia de ciberseguridad. *Revista de Negocios Del IEEM*, 64–65. Retrieved from https://www.haceremprESA.uy/wp-content/uploads/2018/12/IEEM-dic-Emprendimiento.pdf

Fernadez, Y. (2018, October 9). Servidores NAS: qué son, cómo funcionan y qué puedes hacer con uno. Retrieved January 26, 2022, from https://www.xataka.com/basics/servidores-nas-que-como-funcionan-que-puedes-hacer-uno

Fernández, A., García, L., & Garofalo, A. (2018). Propuesta de controles de seguridad para nubes privadas y centros de datos virtualizados. *Telemática*, *17*(1), 56–72. Retrieved from https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/290

Fidias, A. (2017). *EL PROYECTO DE INVESTIGACION FIDIAS ARIAS 7MA EDIC 2016.pdf - Free Download PDF* (7th ed.). Caracas: Episteme. Retrieved from https://kupdf.net/download/el-proyecto-de-investigacion-fidias-arias-7ma-edic-2016pdf_5a1b4afde2b6f5e526da642c_pdf

Guijarro, A., Yepez, J., Peralta, T., & Ortiz, M. (2018). No Title. *Revista Espacios*, *39*(0798 1015), 19–27.

Hernández, A., & Mejía, J. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *Revista Electronica de Computacion, Informatica Biomedica y Electronica*, 1–18.

Hernández, M. (2019, September 2). En América Latina se registran 45 ataques cibernéticos por segundo • Tecnología • Forbes México. Retrieved July 2, 2021, from https://www.forbes.com.mx/en-america-latina-se-registran-45-ataques-ciberneticos-por-segundo/

Herzog, P. (2010). *OSSTMM*. ISECOM. Retrieved from www.osstmm.org

IBM. (2015). Disponibilidad - Documentación de IBM. Retrieved January 26, 2022, from https://www.ibm.com/docs/es/i/7.3?topic=availability-roadmap

IBM. (2021). IaaS-PaaS. Retrieved from https://www.ibm.com/es-es/cloud/learn/cloud-computing-gbl

INCIBE. (2015, May 21). DoS: Capa de Aplicación | INCIBE-CERT. Retrieved September 8, 2021, from https://www.incibe-cert.es/blog/dos-capa-aplicacion

Insurance Journal. (2016, May 24). Cyber Bank Thieves Stole $12M from Ecuador Bank in 2015, Using SWIFT System. Retrieved June 30, 2021, from https://www.insurancejournal.com/news/international/2016/05/24/409577.htm

IONOS. (2018, December 4). SMTP: el requisito para enviar correos electrónicos - IONOS. Retrieved January 26, 2022, from https://www.ionos.es/digitalguide/correo-electronico/cuestiones-tecnicas/smtp/

IONOS. (2020, October 1). SYN flood: métodos de ataque y medidas de protección - IONOS. Retrieved October 4, 2021, from https://www.ionos.es/digitalguide/servidores/seguridad/syn-flood/

Jhony, E., & Alvarado, Y. (2015). LOS DELITOS INFORMÁTICOS Y SU PENALIZACIÓN EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL

ECUATORIANO. *Universidad Politécnica Estatal Del Carchi*, *8*, 171–194.

Juan, M., Luis, M., Carlos, M., & Juan, O. (2008). (PDF) Implementación y mejora de la consola de seguridad informática OSSIM una experiencia de colaboración universidad-empresa. *ResearchGate*, *6*, 29–37. Retrieved from https://www.researchgate.net/publication/279490894_Implementacion_y_mejora_de_la_consola_de_seguridad_informatica_OSSIM_una_experiencia_de_colaboracion_universidad-empresa

Kavanagh, K. M., & Rochford, O. (2015). *Magic Quadrant for Security Information and Event Management Magic Quadrant for Security Information and Event Management Magic Quadrant Figure 1. Magic Quadrant for Security Information and Event Management EVALUATION CRITERIA DEFINITIONS*. Retrieved from http://www.gartner.com/technology/reprints.do?id=1-2JNR3RU&ct=150720&st=sb

La Republica. (2021, March 24). *Aumenta la preocupación por la ciberseguridad en Latinoamérica | La República EC*. Retrieved from https://www.larepublica.ec/blog/2021/03/24/aumenta-la-preocupacion-por-la-ciberseguridad-en-latinoamerica/

Lopez, C. (2021, January 28). ¿Qué es el protocolo ICMP y para qué sirve? - CCM. Retrieved January 26, 2022, from CCM website: https://es.ccm.net/contents/265-el-protocolo-icmp

Miller, D., Harris, S., Harper, A., Vandyke, S., & Black, C. (2010). Security Information and Event Management (SIEM) Implementation. *McGraw-Hill Osborne Media*. Retrieved from https://mhebooklibrary.com/doi/book/10.1036/9780071701082

Montesin, R., Garcia, W., & Rubier, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *Revista Ingeniería Electrónica, Automática y Comunicaciones*, *34*(1), 40–58. https://doi.org/10.1234/rielac.v34i1.152

Montesino, R., Garcia, W., & Porven, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *Revista Ingeniería Electrónica, Automática y Comunicaciones*, *34*(1), 40–58. https://doi.org/10.1234/RIELAC.V34I1.152

Morales, F., Toapanta, S., & Toasa, R. M. (2019). Implementación de un sistema de seguridad - ProQuest. *ARevista Ibérica de Sistemas e Tecnologias de Informação*, *E27*(2020), 553–565. Retrieved from https://www.proquest.com/docview/2385756526/696816F9FCA141D8PQ/1

Müller, A. (2009). *Event Correlation Engine*. 31–57.

Nagios. (2016). Herramientas de monitoreo - GREENCORE SOLUTIONS. Retrieved January 26, 2022, from https://www.greencore.co.cr/herramientas-de-monitoreo.html

Nagios. (2021). Nagios Fusion - Central Monitoring Infrastructure View. Retrieved

January 26, 2022, from https://www.nagios.com/products/nagios-fusion/

NTOP. (n.d.). ntop – High Performance Network Monitoring Solutions based on Open Source and Commodity Hardware. Retrieved June 30, 2021, from https://www.ntop.org/

OpenVas. (n.d.). OpenVAS - Open Vulnerability Assessment Scanner. Retrieved June 30, 2021, from https://www.openvas.org/

OSI. (2018, August 21). ¿Qué son los ataques DoS y DDoS? | Oficina de Seguridad del Internauta. Retrieved October 3, 2021, from Oficina de Seguridad del Internauta website: https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

Quintero, M., & Tovar, S. (2019). Sistema de Gestion de Informacion y Eventos de Seguridad (SIEM. *Tecnologias de Informacion En Eduacacion Superior TIES*, *1*, 30–36. Retrieved from https://www.ties.unam.mx/num02/pdf/num02.pdf

Raudales, C. (2017). La Brecha Existente En La Ciberseguridad En Honduras. *Innovare Ciencia y Tecnología*, 58–73.

RedHat. (2018, March 14). ¿Qué es el cloud computing? Retrieved January 26, 2022, from https://www.redhat.com/es/topics/cloud

Rodriguez, L. (2016). Integración de un sistema de detección de intrusos y un escáner de vulnerabilidades para la detección efectiva de ataques informáticos. *Universidad de Las Ciencias Informáticas*, *9*, 51–69.

Rouse, M. (2019). ¿Qué es Gestión de eventos e información de seguridad (SIEM)? - Definición en WhatIs.com. Retrieved January 26, 2022, from https://www.computerweekly.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM

Snort. (n.d.). Snort Setup Guides for Emerging Threats Prevention. Retrieved June 30, 2021, from https://www.snort.org/documents

TechTarget. (2021). ¿Qué es Fuente abierta o código abierto (open source) ? - Definición en WhatIs.com. Retrieved January 26, 2022, from https://www.computerweekly.com/es/definicion/Fuente-abierta-o-codigo-abierto-open-source

Tom Bergin, & Nathan Layne. (2016). *Special Report: Cyber thieves exploit banks' faith in SWIFT transfer network | Reuters*. London/Chicago. Retrieved from https://www.reuters.com/article/us-cyber-heist-swift-specialreport/special-report-cyber-thieves-exploit-banks-faith-in-swift-transfer-network-idUSKCN0YB0DD

VIU. (2020). Redes de datos, todo lo que hay que saber sobre ellas | VIU. Retrieved January 26, 2022, from https://www.universidadviu.com/ec/actualidad/nuestros-expertos/redes-de-datos-todo-lo-que-hay-que-saber-sobre-ellas