Afinación de reglas en un SIEM para correlacionar los eventos de seguridad del laboratorio de redes convergentes del ITM

Sebastián Rivera Montoya

Carlos Alberto Pérez Cataño

Ingeniería en telecomunicaciones

Director(es) del trabajo de grado

Msc. Héctor Fernando Vargas Montoya

INSTITUTO TECNOLÓGICO METROPOLITANO

2018

RESUMEN

Debido a los grandes avances tecnológicos que se están presentando, las entidades que cuentan con dispositivos informáticos se encuentran altamente vulnerables; ya que ofrecen diversidad de servicios a un alto número de personas y como deber fundamental de estas entidades es evitar los posibles ataques que atenten contra la integridad, confiabilidad y disponibilidad de sus sistemas.

Este proyecto busca apoyarse en la infraestructura que se encuentra ubicada en el laboratorio de redes convergentes del Bloque O del ITM para la configuración y afinación de un correlacionador de eventos de seguridad – SIEM, el cual se encuentra enfocado hacia la seguridad informática, validando los routers, servidores y dispositivos de seguridad que se encuentren en el laboratorio, con el fin de ofrecer un mecanismo de monitoreo proactivo de las diferentes amenazas que puedan generarse en las instalaciones y equipos (físicos y/o virtuales) del laboratorio, ya que es una área que maneja un alto flujo de información. Para la implementación de este proyecto se decide utilizar la herramienta OSSIM de Alienvault, la cuenta con una licencia Open Source y que cumple con las características necesarias para gestionar los eventos de seguridad que suceden en los dispositivos de red; permitiendo la recolección de logs, alertas sobre posibles vulnerabilidades, configuración de reglas, entre otras funcionalidades.

El SIEM debe ser evaluado para garantizar su óptimo funcionamiento y para ello se llevaron a cabo una serie de pruebas explotando las vulnerabilidades de los dispositivos, con las diversas aplicaciones que dispone la herramienta Kali Linux; es necesario analizar los logs que arrojaron los dispositivos al servidor SIEM para ver la información del ataque.

Palabras clave: Logs, SIEM, Open Source, vulnerabilidades, alertas, correlación de eventos, dispositivos de red y amenazas.

RECONOCIMIENTOS

Queremos reconocer un especial agradecimiento al profesor Héctor Fernando Vargas, el cual fue un excelente asesor y director de este trabajo. Su paciencia, dedicación, interés y apoyo fueron primordiales para el logro de este objetivo.

También reconocer la excelente labor que tuvieron los compañeros Christian Gaviria y Steven Urrego por facilitarnos las herramientas y accesos necesarios en los espacios requeridos.

A la institución universitaria ITM por facilitarnos el espacio del laboratorio de redes convergentes ubicado en el Bloque O

Finalmente, a nuestras familias por su constante apoyo moral y comprensión en todo el transcurso del proyecto.

ACRÓNIMOS

OSSIM*:* Open Source Security Information Management.

LOG: Archivo de texto que describe un acontecimiento en algún tipo de sistema.

HIDS: Host-based Intrusion Detection System o Sistema de detección de intrusos de Host.

NIDS: Network Intrusion Detection System o Sistema de detección de intrusos en una Red.SIEM: Security Information and Event Management.

MiM: Men In The Middle o hombre en el medio.

SNMP: Simple Network Managment Protocol o Protocolo simple de administración de red.

DoS: Deny Of Service o Denegación de servicio.

SYSLOG: mensaje de registro o Tambien considerado metodo de transporte de logs.

HOST: Dispositivo utilizado para proveer servicios o sacarle utilidad de la red a la que este conectado.

PLUGIN: Es un complemento especifico para un tipo de Sistema o aplicación, el cual mejora su funcionamiento.

AGENTE: Son programas que se ejecutan en un dispositivo para cumplir un proposito en especifico.

Mikrotik: Porveedor de dispositivos de red.

UDP: User Data Protocol o Protocolo de Datagrama de Usuario.

Router: Dispositivo que proporciona conectividad.

Nmap: Es una herramienta muy utilizada para mirar el estado de los puertos que estén abiertos en los dispositivos

TCP: Transmision Control Protocol o Protocolo de Control de Transmisión.

Open VAS: Es utilizado para hacer un escaneo de vulnerabilidades a los hosts involucrados en la red, esta información se almacena en el base de datos de OSSIM.

OSSEC: Es una herramienta muy potente ya que provee un estudio de logs, verificación de integridad de archivos, monitoreo de políticas, monitoreo de alertas, además cuenta con una respuesta en real time.

SO: Sistema operativo.

Hipervisores: Plataforma que sirve para controlar la virtualización de diversos SO al mismo tiempo.

Hping3: Herramienta de que se utiliza desde la línea de comandos de Linux que nos permite modificar y analizar paquetes; usado para realizar ataques DoS/DDoS.

Ettercap: Herramienta de Linux para realizar ataques de hombre en el medio ya que permite interceptar conexiones en vivo.

SSH: Es un protocolo de administración remota para sistemas Linux, es decir, permite a los usuarios controlar y modificar sus servidores o equipos que tengan habilitado este protocolo.

TELNET: Protocolo para la administración de dispositivos remotamente.

Putty: Es un emulador de una terminal que soporta protocolos como SSH, Telnet, entre otros.

Rsyslog: Es un sistema de procesamiento de registros.

Netflow: Es un protocolo de red que fue desarrollado por Cisco con el fin de poder recolectar información sobre tráfico IP.

Plugin: Es un complemento.

Open Source: Licencia gratuita de algún software.

TABLA DE CONTENIDO

Tabla de contenido

TABLA DE FIGURAS

LISTA DE TABLAS

1. INTRODUCCIÓN

1.1 Generalidades

1.1.1 Pertinencia

Un ambiente informático está compuesto de varios dispositivos de red y sistemas de procesamiento, los cuales generan logs. Estos Logs se componen de información que describe la acción que se está realizando en el dispositivo.

Para muchas de las empresas sean grandes o pequeñas, estos dispositivos representan una gran importancia debido a que ellos manejan información que es valiosa. Viéndolo desde un punto de vista más analítico y enfocado hacia la protección de estos mismos, se busca un tipo de dispositivo que de alguna manera este centrado para custodiar la seguridad de los mismos. De esta manera se pueden tomar medidas de protección y anticiparse a posibles ataques informáticos que puedan ocasionar algún tipo de daño que afecte la empresa.

1.1.2 Justificación

La información digital es considerada un bien intangible de cada compañía, que representa un valor muy importante. Esta información circula a través de dispositivos de red y de procesamiento, los cuales se encargan de enviarla y reenviarla según la petición de cada usuario y estando en manos equivocadas puede ser perjudicial, causando daños que representen posibles pérdidas. Pero adicional a esto, con el aumento de la tecnología, se hace evidente el aumento de los ataques informáticos y los riesgos que pueden presentarse en la no protección adecuada de la información. Estos ataques se dan debido a la exposición de la información, la cual personas con fines malignos pueden ocasionar alteraciones de la disponibilidad e integridad en los servicios que ofrecidos.

Los registros de Logs o auditorias en los sistemas son los registros diarios de cada uno de los dispositivos que conforman una red de datos van generando, debido a que estos

registros pueden significar varias cosas, algunas como: accesos a un dispositivo, una autenticación fallida, cambios de reglas, autenticación o acceso por algún tipo de servicio bien sea Telnet o SSH, entre otros. Pero si miramos más a fondo sabemos que no todos los Logs representan una importancia a la hora de implementar una seguridad, por lo que se debe fijar más la atención en los Logs que representen un valor más crítico y que pueden dar pie a proyectar que existe algún tipo de vulnerabilidad. Esto se hace con el fin de anticipar algo que pueda generar un daño o impacto en el sistema.

Actualmente existe una herramienta muy eficiente que se puede implementar para la materia prima que tenemos: logs. Esta herramienta se llama SIEM, que su motor principal de funcionamiento es la recolección y correlación de eventos de seguridad y funciona de una manera muy efectiva debido a que se encarga de recolectar topos los tipos de Log que son generados por los dispositivos que se encuentran alojados en una red. Con base a esta recolección se pueden crear unas reglas y políticas que ayuden al gestionamiento de las posibles vulnerabilidades que puedan tener. Claro está según como este expuesto el dispositivo y también la importancia que represente en la red.

1.1.3 Problema abordado

La tecnología es una herramienta de la cual se valen muchas de las empresas y personas para proveer sus servicios bien sea a través de un computador o un celular. Por ende, esta herramienta maneja una gran cantidad de flujo de datos y es necesario que el ambiente en donde este circulando dichos datos sea un entorno seguro. Por esto la seguridad informática es un tema que ha venido cobrando una alta relevancia en el mundo de la tecnología, debido a que es un mundo con demasiados campos por explorar, ya que es algo que se convirtió en una necesidad para todo tipo de entorno en donde se manejen dispositivos tecnológicos y más aún cuando la mayoría de las empresas están expuestas a posibles amenazas que atenten contra la disponibilidad, confidencialidad e integridad de la información.

Según las estadísticas reveladas en abril de 2018 por (CERTuy, 2018) - Centro Nacional de Respuesta a Incidentes de Seguridad Informática demuestran la cantidad de incidentes

informáticos (1684) de forma semestral, los cuales fueron puestos en un orden de jerarquía según su grado de gravedad.

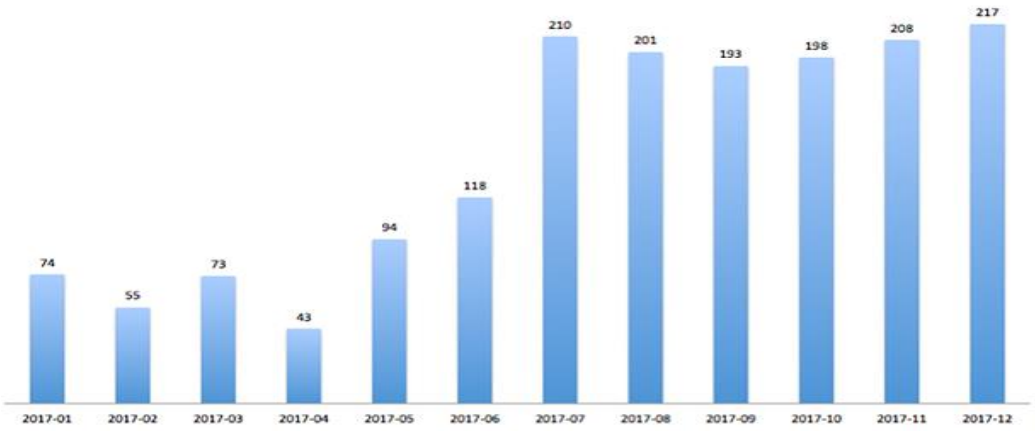


*Ilustración 1.*Estadísticas de incidentes informáticos, tomado de*: https://www.intradosti.com/single-post/2018/04/20/Estad%C3%ADsticas-2017-incidentes-de-seguridad-inform%C3%A1tica*

Es evidente que desde un principio se ve un aumento demasiado notable de como incrementan las amenazas informáticas. También es importante destacar cuales fueron los ataques atendidos en base a estas estadísticas de la gráfica anterior, lo cual nos lleva a un análisis más a fondo y detallado de que fue lo atendido:

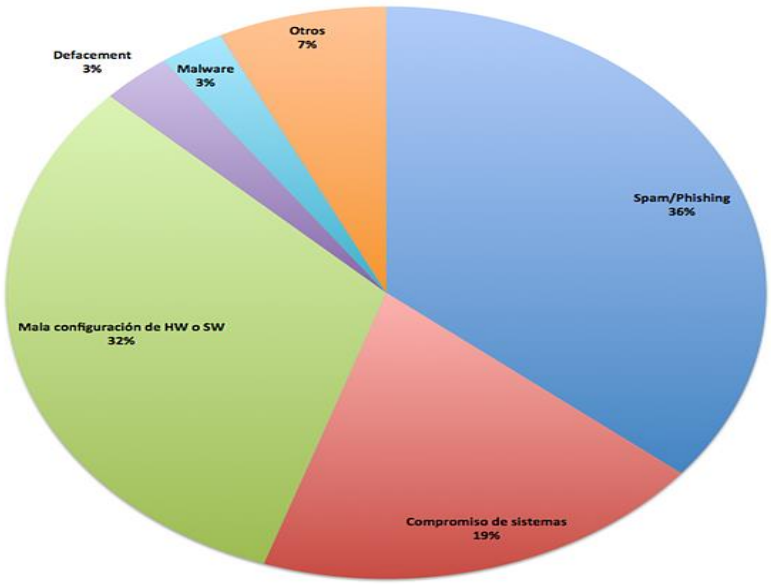


*Ilustración 2.*Ataques informáticos atendidos, tomado de: https://www.intradosti.com/single-post/2018/04/20/Estad%C3%ADsticas-2017-incidentes-de-seguridad-inform%C3%A1tica

tomando como base las dos graficas anteriores, podemos pensar en que se puede hacer para mitigar o por lo menos poner un alto a este crecimiento exponencial de ataques informáticos. Aunque si miramos desde un punto de vista más analítico no todos los ataques informáticos son perpetrados por personas externas a la empresa, sino que también dependen del mismo cuidado de la persona que esté a cargo de las configuraciones de los dispositivos, ya que de ellas dependen que no dejen ventanas o puertas abiertas a personas que pueda ocasionar posibles daños.

No solo las empresas son las que se ven expuestas a un peligro tan abundante como lo es un ataque informático. También universidades y personas que manejen hasta el más mínimo flujo de datos se pueden convertir en el objetivo de un atacante con fines maliciosos. De esta manera, el laboratorio de redes convergentes del Bloque O ubicado en el Instituto Tecnológico Metropolitano sede Boston, es donde se encuentra alojada toda la infraestructura física/virtual principal de todo el bloque, ya que está compuesta de servidores, enrutadores, Acces Point, switch, portátiles, entre otros dispositivos que proveen servicios a muchos estudiantes, profesores y personas externas a la universidad.

En vista de la gran importancia que representa el laboratorio de redes convergentes y la gran cantidad de dispositivos que cuenta con él, se ve la necesidad de implementar una herramienta que ayude al aseguramiento y monitoreo de estos mismos; debido a esto se encontró como una posible solución a implementar en dicha infraestructura un SIEM (Security Information and Event Managment) que funcione como un correlacionador de eventos de seguridad, ya que gracias a las reglas o directivas de correlación se puede evaluar de manera más crítica los diferentes eventos que se puedan presentar en los dispositivos, teniendo un criterio más acertado de cuando se puede estar vulnerando o atacando algún activo que pertenezca a esta área, ya que este SIEM mantiene en constante monitoreo alertando cuando encuentra algo anómalo.

1.2 OBJETIVOS

Los siguientes son los objetivos planteados en el proyecto:

1.2.1 General

Diseñar una estructura de reglas de correlación de eventos de seguridad en un SIEM para la detección temprana de eventos de seguridad que puedan impactar en los elementos tecnológicos (físicos y/o lógicos) del laboratorio de redes convergentes del bloque O.

1.2.2. Específicos

- Identificar los diferentes componentes informáticos, de red y de seguridad en el bloque O que deban ser potencializados y/o monitoreados.
- Examinar que reglas de correlación de eventos de seguridad disponibles y cuales se pueden usar o crear.
- Diseñar el SIEM con las reglas de correlación de eventos, considerando el software existente o uno nuevo a implementar, así como la ejecución de diferentes pruebas de seguridad.
- Documentar las pruebas, ensayos y correcciones que se realicen en el transcurso del proyecto.

1.3. ORGANIZACIÓN DE LA TESIS

Inicialmente el desarrollo y organización de la tesis estará dividido en dos partes. La primera estará compuesta del marco teórico donde se dará a conocer sustentos investigativos basados en diferentes fuentes de información las cuales hacen relación a la ejecución del SIEM como correlacionador de eventos de seguridad, haciendo un análisis donde se evidencia la importancia de este mismo. Seguidamente la segunda parte se basa de la metodología PHVA, la cual está apoyada de 4 fases, las cuales se presentan a continuación:

Tabla 1.Fases de procedimiento de la tesis (Elaboración propia)

No.	Fase
1.	En esta fase se hará un levantamiento de información con respecto al inventario de los diferentes elementos computacionales como servidores, equipos de comunicaciones, soluciones de seguridad (IDS/IPS, Firewall, WAF, SIEM, etc.) en el bloque O. Así mismo, se determinarán los servicios que allí se prestan y los diferentes ataques informáticos que pueden sufrir, para ello, se hará una tabla entre los servicios vs. Ataques posibles y el nivel de riesgo que puedan tener (alto, medio o bajo), el nivel de riesgo será determinado por el vector de ataque, la probabilidad de que ocurra y el impacto que pueda genera.
2.	En esta fase se determinará, acorde al análisis anterior, cuáles son los servicios a ser monitoreados y correlacionados. Así mismo, se revisarán las diferentes reglas de correlación de eventos que puedan estar disponibles a través de la búsqueda en bases de datos especializadas y consulta con expertos en el área de seguridad, se hará un levantamiento de información de reglas (básica y avanzadas) dependiendo de los servicios seleccionados, aquellas reglas que los expertos indiquen son importantes para la seguridad y no existe una regla creada, se creará.
3.	Realizar el diseño e implementación con la arquitectura SIEM (sino existe) y la configuración o afinación de las diferentes reglas a implementar (ya existentes y/o creadas). Así mismo, se ejecutarán las diferentes pruebas de validación de funcionamiento de las reglas, realizando diferentes ataques informáticos y tabulando el comportamiento de la correlación de eventos, con ello, reducir los falsos positivos.
4.	Documentar todas las pruebas realizadas y se generan las conclusiones respectivas acerca del funcionamiento de la afinación de la correlación de eventos. Paralelo a todas las fases, se hará la construcción del documento final.

Seguidamente se hará el análisis respectivo de las pruebas realizadas en el SIEM, con las distintas herramientas que se tengan a la mano.

Finalmente estará compuesto de la sección de: resultados y discusiones, conclusiones, recomendaciones, trabajo futuro, referencias y paso a paso de las configuraciones realizadas para la instalación del OSSIM como SIEM, configuraciones realizadas para las reglas de correlación y para los dispositivos.

2. MARCO TEÓRICO

SIEM (Security Information Event Managment) hace una unificación de lo que es SIM (Security Information Managmet) y SEM (Security Event Managment), además que posee distintos atributos que lo hacen una herramienta de seguridad informática muy potente como se muestra en la Ilustración 3, haciendo que se pueda centralizar y analizar de manera adecuada un instrumento que no es muy mencionado y utilizado en la red llamado log o evento. Un evento o log podemos definir como tipo de registro que describa algún acontecimiento del sistema en cuestión.

Ilustración 3.Características de un SIEM, tomado de: https://codingcompiler.com/siem-tools-list/

Además de esto un SIEM funciona de manera centralizada operando en una arquitectura tipo estrella, por cómo se puede ver en la siguiente ilustración:

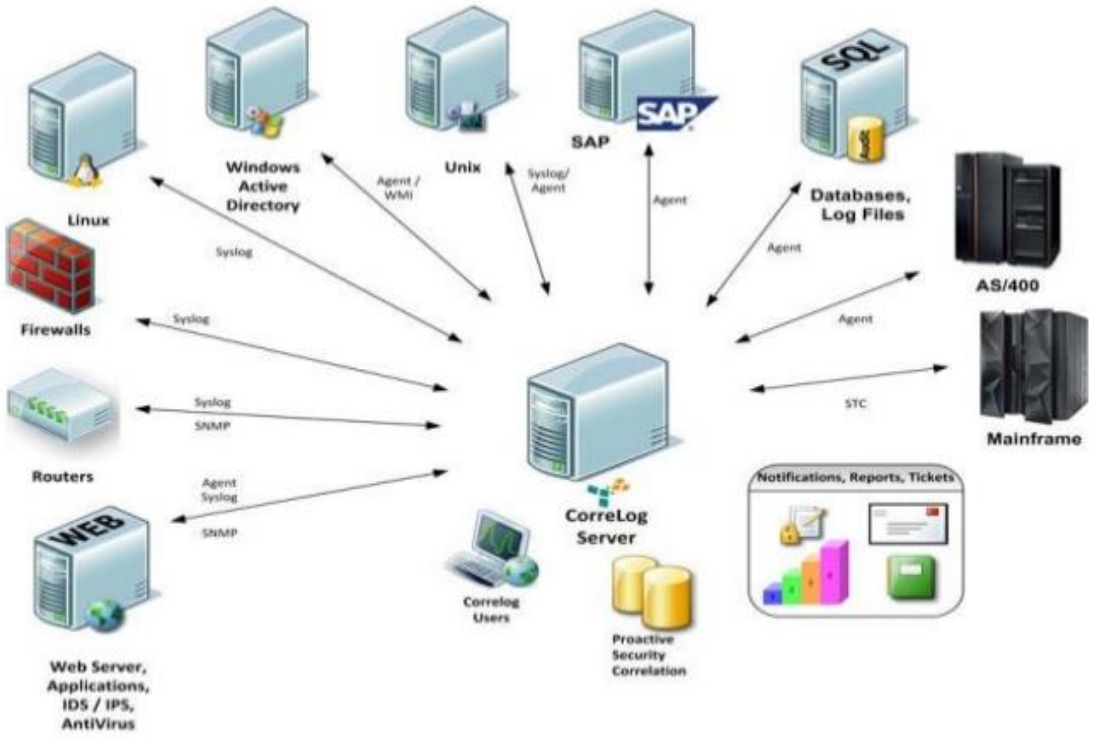


Ilustración 4. Arquitectura de un SIEM, tomado de: http://www.portalticsecurity.com/catalogo-productos/seguridad-informatica/seguridad-endpoint/mcafee-siem.html

Según la gráfica anterior se puede observar que el SIEM se encuentra en la parte central de toda la distribución de la red, donde todos los dispositivos que se encuentran alojas en ella le envían mensajes de tipo syslog (mensaje de registro o método de transporte de log), bien sea por una configuración aplicada en cada dispositivo o también por la ejecución de un agente (Son programas que se ejecutan en un dispositivo para cumplir un propósito en específico) en el sistema. Estos syslog son también es definido como todo suceso que pueda ocurrir en un ambiente, para este caso informático, además que es considerado como el componente principal con el cual podrá ponerse en función el motor de correlación.

Los componentes que hacen parte de una red de datos, sin excepción alguna, generan una gran variedad de eventos los cuales algunos pueden tener información de suma importancia. Estos eventos necesitan ser de alguna forma monitoreados y administrados para poder tener gestión y control sobre estos.

Hay que tener en cuenta algo que se presenta, si bien se había indicado que los logs es algo natural que cada dispositivo genera, bien sea configurado o programado a través de un agente, en algunas ocasiones éstos logs no pueden ser leídos o procesados por múltiples razones: No tienen la información que se requiere de seguridad, hay reglas de firewall que impiden el tráfico, aumento en el procesamiento debido a la activación de logs, entre otros. Para estos eventos existen métodos de transporte los cuales hasta el momento son los más utilizados y han representado una buena eficiencia, los cuales se pueden ver a continuación:

- Syslog: según (Munera, 2007), syslog "Es un sistema de logs que se encarga principalmente de la administración de log", estos mensajes syslog son enviados mediante el puerto 514 de UDP (Protocolo no orientado a la conexión), en vista que estos mensajes no se encuentran cifrados, están expuestos a personas con fines maliciosos.
- SNMP (Simple Network Managment Protocol): es un protocolo que da paso a los administradores de red poder tener gestión de los dispositivos conectados a la red de datos y poder realizar un diagnóstico en base a dicho control. Para este protocolo hay dos maneras de poder trabajarlo, una es por Traps, el cual consiste en mensajes que envían (logs) los dispositivos a una dirección en específico, la segunda es Polling la cual se apoya enviando consultas bien sean de una forma activa o bajo demanda. (Pardo, 2018)

De esta forma las empresas, entidades gubernamentales o instituciones educativas, buscan obtener una seguridad la cual pueda brindar una vista completa del sistema. Según(S. Sandeep Sekharan, 2017), inicialmente esta herramienta (SIEM) funciona haciendo una recolección de datos que son efectuados por una institución, empresa o compañía desde cualquier punto de sí misma, haciendo de esta manera un análisis para detectar una posible vulnerabilidad. Esta recolección de datos se hace de una manera en donde se almacena y se administra la información, también permite funciones de monitoreo (Real Time) y correlación de registros. Estos SIEM, después de realizar el procesamiento y almacenamiento debido, analizan los datos para producir alertas acerca de los

descubrimientos irregulares que fueron detectados, de esta manera es mucho más fácil mitigar un ataque ya que se está notificando a tiempo cuando están sucediendo las cosas.

Así mismo, (S. Sandeep Sekharan, 2017) SIEM incorpora nuevas formas de análisis para interpretar los datos, de esta manera se puede hacer una prevención de tal forma que no generen daños en el sistema, minimizando de esta manera ciberataques, intrusos y vulnerabilidades. También este tipo de solución integra diversidad de capacidades haciéndola muy útil debido a que se puede desempeñar en diferentes áreas, estas son:

- Perfiles de comportamiento: Consiste en la creación de un perfil de actividad normal el cual se encargará de vigilar y aprender el comportamiento o actividad habitual de cada usuario en el espacio que se desempeñe, es decir: accesos a servidores, flujos de tráfico, manejo de información, entre otros.
- Monitoreo de seguridad en tiempo real: Debido a que un SIEM puede proporcionar un almacenamiento y registro de manera centralizada en una institución, organización o empresa, también tiene la capacidad de brindar información acerca de la actividad que se esté realizando en el momento bien sea por un usuario o amenaza, dependiendo de esta se toman medidas para mitigar la amenaza al máximo.
- Monitoreo de datos y usuarios: Esta parte funciona como una estrategia de seguridad debido a que realiza una autenticación con el usuario buscando de esta manera los lugares, archivos y permisos donde tiene el acceso; cualquier cambio o alteración se considerará como un comportamiento anormal creando de esta manera una alerta.
- Monitoreo de aplicaciones: Sabemos que una de las debilidades de las aplicaciones es cuando reportan errores inesperados o empiezan con un funcionamiento anómalo (siendo de los casos más comunes un poco lento). SIEM incorpora este tipo de monitoreo para la supervisión y análisis de la capacidad de las aplicaciones, debido a que una vulnerabilidad involucrando estas aplicaciones es mediante ataques dirigidos.

- Inteligencia de amenazas: Esta capacidad de la SIEM pone en contexto acerca de los diferentes ataques que pueden suceder en cualquier ambiente informático. De esta manera es más fácil comprender estas amenazas o vulnerabilidades, algunas de ellas son: sploits, metasploit y vulnerabilidad del día cero. (S. Sandeep Sekharan, 2017)

Todas las infraestructuras de hoy en día son diferentes, siendo unas más críticas que otras, debido a esto, se recurre a uno de los pilares fundamentales en la arquitectura SIEM llamado motor de correlación, el cual cumple una función muy importante de brindar información acerca de la seguridad interna de los eventos actuales. Debido a que el motor de correlación es de gran importancia porque debe procesar grandes cantidades de información se recurre a motores de correlación que se basan en reglas de código abierto.

Existen varios tipos de correlación los cuales pueden desempeñarse en base a las similitudes, conocimiento y estadísticas.

- Correlación basada en similitud: Consiste en hacer una comparación respecto a las demás alertas que estén sucediendo.
- Correlación basada en el conocimiento: Para este tipo de correlación se debe tener un conocimiento base de la amenaza.
- Correlación estadística: Para esta ocasión no depende de un conocimiento existente, sino que se basa de las actividades ya detalladas.

Entendiendo la información anterior se puede decir qué un SIEM es una herramienta con una amplia gama de características que pueden funcionar en un ambiente informático en plenas condiciones. En base a esta herramienta, muchas de las empresas que buscan innovar con esta herramienta haciendo de ellos un diseño propio de lo que puede ser un SIEM, sin hacer alteraciones que cambien su enfoque general. Es importante aclarar que cada SIEM es acoplado según las necesidades de cada persona o empresa.

A continuación, se presentan algunas de las herramientas que pueden ser implementas como SIEM. Además de sus funcionalidades.

Tabla 2. Herramientas SIEM (Elaboración propia)

HERRAMIENTAS SIEM			
SIEM	FABRICANTE	TIPO DE LICENCIA	DESCRIPCIÓN
IBM QRadar Security Intelligence Platform	IBM	Paga/libre	"SIEM detecta anomalías, descubre amenazas avanzadas y elimina falsos positivos. Consolida datos de eventos de registro y de flujo de red de miles de dispositivos, puntos finales y aplicaciones distribuidos por toda una red. Después, utiliza un avanzado motor de Sense Analytics para normalizar y correlacionar estos datos, e identifica las violaciones a la seguridad que requieren investigación. Como opción, puede incorporar IBM X-Force® Threat Intelligence, que suministra una lista de direcciones IP potencialmente maliciosas, incluyendo hosts de malware, fuentes de spam y otras amenazas. QRadar SIEM está disponible en las instalaciones y en un entorno de nube." Tomado de: https://www.ibm.com/co-es/marketplace/ibm-qradar-siem
Splunk SIEM	Splunk Enterprise Security	Paga/libre	"Splunk ES, es un SIEM basado en análisis que permite a los equipos de seguridad detectar y responder a ataques internos y externos, y simplificar la gestión de amenazas: centraliza y agrega todos los eventos relevantes para la seguridad a medida que se generan desde su origen. Además, admite una variedad de mecanismos de recepción / recolección, y proporciona búsquedas e informes ad hoc para análisis de incumplimiento". Tomado de: https://www.esecurityplanet.com/products/splunk-enterprise-security-siem.html
Micro Focus SIEM	ArcSight ESM	Paga	Este SIEM se caracteriza por responder más rápido las amenazas que puedan tener una evolución. Tiene la capacidad de correlacionar hasta 100.000 eventos por segundo, además de resolver un conjunto más amplio de casos de seguridad. Posee correlación distribuida, vista de grupo, entre otros.

Trustwave SIEM	Trustwave	Paga/libre	Trustwave ofrece una herramienta SIEM con la capacidad de centralizar la gestión de los registros, correlación de datos. Además, posee dos versiones de SIEM, una es LME (Log Managment Enterprise) es un poco más básico ya que no requiere tantos recursos, y además que es alojado en la nube. el otro SIEM es el SIEM Enterprise que es un poco más robusto, tiene una configuración centralizada.
OSSIM SIEM	Alienvault	Paga/libre	OSSIM es una herramienta muy potente y con muchas capacidades para desempeñarse como SIEM. Tiene dos versiones la cual una es libre llamada OSSIM, cuenta con capacidades de: descubrimiento de nuevos activos, evaluación de vulnerabilidades, detección de intrusos, control de comportamiento, recibir información en real time, implementación de reglas de correlación, estadísticas acerca de los eventos y alertas que suceden en el momento, entre otras más. La otra que es paga llamada USM Anywhere, cuenta con la capacidad de detección de amenazas centralizadas y respuestas a incidentes en diferentes entornos como: nube, infraestructura local y aplicaciones en la nube. También posee gestión de registros para el cumplimiento continuo y las investigaciones forenses, detección avanzada de amenazas con alarmas prioritarias en tiempo real, entre otras más que la hacen una herramienta demasiado completa. Tomado de: https://www.alienvault.com/products/ossim
FortiSIEM	Fortinet	Paga	Posee el autodescubrimiento de activos, rápidas integraciones y escalabilidad, flujo de trabajo automatizado, plataforma unificada. También viene con 3 versiones de SIEM, los cuales son: FortiSIEM 500F tiene la capacidad de procesar 5000 eventos por segundo y tiene una capacidad de almacenamiento de 3 TB, FortiSIEM 2000F tiene la capacidad de procesar 15000 eventos por segundo y tiene una capacidad de almacenamiento de 36 TB, por último, el FortiSIEM 3500 F el cual dobla la capacidad de procesamiento de eventos llevándolo a un total de 30000 por segundo y con una capacidad de almacenamiento de 72 TB

BlackStratus SIEM	BalckStratus	Paga	BalckStratus SIEM tiene un soporte multi-tenancy, visualización de ataques en tiempo real, correlación de vulnerabilidades, arquitectura avanzada, además de herramientas para informes ISO, PCI, HIPAA, SOX.
EventTracker SIEM	EventTracker	Paga	Alertas en tiempo real a incidentes, búsqueda de análisis forense, detección y respuesta a amenazas en el punto final análisis de comportamiento y correlación, comportamiento de amenazas.
Solarwinds SIEM	Solarwinds	Paga/libre	El SIEM que provee SolarWinds provee la facilidad de usar registros de seguridad para la solución, detección y cumplimiento de problemas.

Teniendo esta información, se puede observar que en la tabla anterior están algunos de los SIEM más relevantes del mercado.

El Cuadrante Mágico de Gartner, es una herramienta muy productiva utilizada para el mercadeo tecnológico, además teniendo como objetivo principal ofrecer una ayuda para poder determinar de una manera más rápida que tan fiables y tan bien posicionados están las empresas con las que el usuario quiere adquirir el servicio. El cuadrante mágico de Gartner está representado de una manera gráfica el cual se compone de dos ejes que se cruzan (se puede hacer la similitud de un plano cartesiano) y cuatro cuadrantes. Cada uno de los ejes tiene una representación básica, el eje vertical simboliza el conocimiento del mercado y el horizontal hace referencia a la capacidad de ejecución por parte de los proveedores. Ahora los cuadrantes que lo componen se definen de la siguiente manera:

Ilustración 5. Cuadrante mágico de Gartner, tomado de: http://www.gb-advisors.com/es/cuadrante-de-gartner/

- Retadores o aspirantes: Es donde se ubican las empresas que brindan buenos productos, pero en el momento que surge una solicitud o petición especifica del mercado no tienen la capacidad de ofrecer variedad herramientas para poder participar de la solicitud lanzada. Teniendo esto claro y desde un punto de vista profesional las empresas que aparecen en este cuadrante son un poco limitadas.
- Jugadores de nicho: En este recuadro es donde se agrupan los interesados, pero que debido a la calificación que le es dada no cumplen con la debida lista de cotejo para calificar o ascender a otra categoría, aunque siguen cumpliendo son ciertos requerimientos.
- Visionarios: Los visionarios tienen aspectos similares a los que están ubicadas en el recuadro de los lideres ya que pueden pronosticar necesidades que pueda tener el mercado tecnológico en el momento, pero no cuentan con las herramientas necesarias para suplir las necesidades a nivel general.
- Líderes: Este compuesto por dos partes, los proveedores de soluciones y servicios de tecnología informática. Este recuadro se puede decir que es la más alta categoría en el cuadro mágico de Gartner debido a que cumplen con una lista especifica que agrupa una visión de mercado, además de la habilidad y herramientas que cuentan para la ejecución y la amplia gama de soluciones. (Mendoza, 2017)

En la siguiente ilustración se muestra la evaluación del cuadrante mágico de Gartner para los SIEM en el año 2017

*Ilustración 6.*Cuadro Mágico de Gartner para los SIEM año 2017. Tomado de: https://es.logrhythm.com/2017-gartner-magic-quadrant-siem-report-a/

Luego de analizar y evaluar la información presentada en la *Tabla 2. Herramientas SIEM (Elaboración propia)*, además de analizar también la *Ilustración 6.Cuadro Mágico de Gartner para los SIEM año* 2017. Tomado de: https://es.logrhythm.com/2017-gartner-magic-quadrant-siem-report-a/, podemos que notar que algunos de los proveedores descritos anteriormente aparecen en ciertos campos de los recuadros del cuadro de Gartner. También para la elección del SIEM a implementar se tomó en cuenta la documentación reciente que se tuviera acerca de este, así como foros, documentación, tutoriales, atención en línea de

dudas y la posibilidad de instalar o tener una versión Free, dado el proceso académico que se desarrolló. Para ello se eligió trabajar con el software de Alienvault OSSIM.

Alienvault OSSIM

OSSIM (Open Source Security Information Managment), es un appliance basado en Debian, creado por Alienvault, el cual trabaja bajo una licencia Open Source es decir libre y otro licenciado llamada Alienvault USM Anywhere. Hay que recalcar que la versión gratuita no cuenta con las mismas características que cuenta USM Anywhere debido a que lo limita un poco en cuanto a funcionamiento, almacenamiento y soporte. Sin embargo, OSSIM, sigue siendo una herramienta SIEM de gran utilidad ya que se acomoda a las necesidades de empresas no tan grandes con pocos recursos a monitorear.

OSSIM, cuenta con una gran cantidad de herramientas para desempeñarse como SIEM, diseñado principalmente para ser alojado en una infraestructura de red físico/lógica con el fin de ayudar a fortalecer la seguridad de la red, también para tener una detección temprana y a tiempo de intrusos, de esta manera ser un poco más anticipado ante cualquier anormalidad.

OSSIM cuenta con una agrupación de características que lo hacen muy robusto en cuanto a la correlación de eventos, estas son:

Tabla 3. Características OSSIM

Tomado de: https://www.alienvault.com/products/ossim/compare.

Características OSSIM	
Herramientas	Descripción
Disponibilidad del producto	Descarga de software de código abierto
Precio	Open Source
Control de seguridad	Entornos físicos y virtuales en las instalaciones
Descubrimiento de activos e inventario	APLICA
Evaluación de vulnerabilidades	APLICA

Detección de intrusos	APLICA
Control de comportamiento	APLICA
Correlación de eventos SIEM	APLICA
Apoyo comunitario a través de foros	APLICA
Open Threat Exchange	APLICA

Teniendo esto claro es muy importante indicar cómo funciona la arquitectura de OSSIM, ya que debido a esta es donde se entiende cuáles son los componentes principales por donde se puede dar la correlación de eventos.

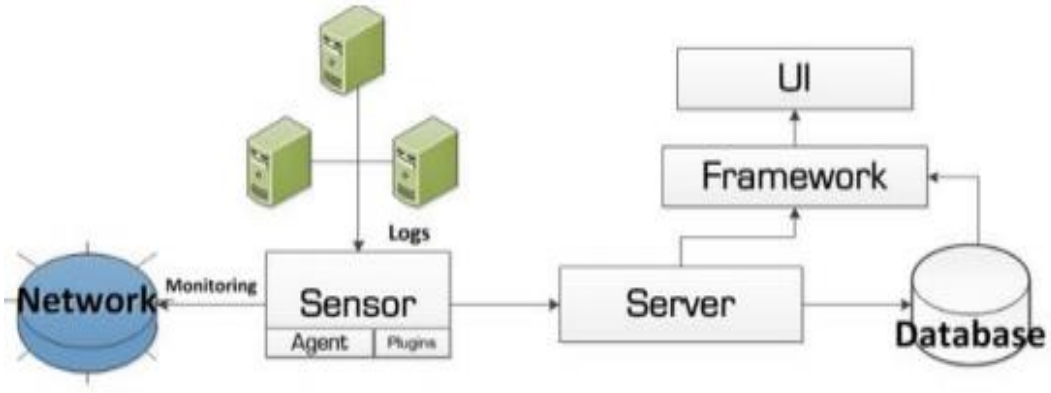


*Ilustración 7.*Arquitectura OSSIM (Arango, 2016)

Como podemos observar la *Ilustración 7.Arquitectura OSSIM*, nos muestra una información de gran valor para entender cómo funciona OSSIM, la cual la podemos desglosar de la siguiente manera:

- Como bien podemos observar el sensor, es el encargado de recolectar los logs de los diferentes dispositivos que se encuentran alojados en una red de datos y estos son enviados hacia el servidor OSSIM. A su vez el sensor puede actuar como un agente que se apoya en los plugin para el envío de la información.
- El servidor OSSIM es donde se alojan las herramientas principales del SIEM que son la correlación de eventos, configuración de reglas o directivas, escaneo a la red monitoreada, entre otros. Además, está compuesto por un Framework que es

donde se alberga la página o interfaz de usuario. Por medio de esta interfaz de usuario es donde se pueden hacer todas las configuraciones pertinentes a la implementación que se quiera hacer con el SIEM. También la base de datos que es donde se almacenan los eventos que llegan hacia este servidor, el inventario de todos los dispositivos monitoreados, entre otros.

Por temas de licencia hay algunos sensores los cuales no aparecerán activos en la plataforma de la interfaz de usuario. Debido a esto hay varios sensores gratuitos de los cuales nos podemos valer para el funcionamiento correcto del SIEM. Algunos de estos sensores son:

- Snort: Es uno de los más usados en este ambiente, funciona como un IDS, además que se encuentra integrado en OSSIM y tiene la capacidad de proveer alertas que estén relacionadas con ataques referentes a la red.
- Suricata: También funciona como IDS, compatible con las reglas del Snort, pero si ponemos en comparación Suricata y Snort, Suricata lleva una gran ventaja ya que puede funcionar como multihilo, es decir que soporta varios procesamientos a la vez. Mientras que Snort solo funciona con un hilo.
- PADS: Es un sistema utilizado para la detección de activos en la red, la cual hace un monitoreo silencioso en todo el tráfico que se esté transportando por la red, además de que hace un registro acerca de los servicios y host involucrados. De esta manera estos datos pueden ser monitoreados por OSSIM para que se puedan detectar alertas que identifiquen un comportamiento anómalo.
- Nmap: Es una herramienta muy utilizada para mirar el estado de los puertos que estén abiertos en los dispositivos, ya que por dichos puertos se pueden filtrar algún tipo de malware o también puede servir como una puerta abierta para el atacante.
- OpenVAS: Es utilizado para hacer un escaneo de vulnerabilidades a los hosts involucrados en la red, esta información se almacena en el base de datos de OSSIM.
- OSSEC: Quizás es el agente más utilizado por OSSIM ya que utiliza un sistema HIDS (Host-based Intrusion Detection System). Es una herramienta muy potente ya que

provee un estudio de logs, verificación de integridad de archivos, monitoreo de políticas, monitoreo de alertas, además cuenta con una respuesta en real time. También ayuda a brindar una protección hacia el mismo OSSIM. (Arango, 2016)

Luego de hacer una investigación exhaustiva encontramos un documento de un caso de estudio para Maestría en Redes de Comunicaciones, el cual es titulado como: Análisis y Selección de una herramienta para administración y obtención de información de eventos críticos de seguridad informática para la infraestructura del Ministerio de Telecomunicaciones y de la Sociedad de la información – MINTEL. Este proyecto tenía como objetivo general "Analizar herramientas de software licenciadas o libres para la implementación de un sistema de seguridad de la información y gestión de eventos - SIEM y seleccionar la de mejor desempeño para la infraestructura del Ministerio de Telecomunicaciones y de la Sociedad de la Información" (Boada, 2016). Teniendo en cuenta este objetivo a lo largo del trabajo proponen varias alternativas para la implementación. Dentro de los seleccionados esta Alienvault OSSIM como software Open Source, Splunk y McAfee Enterprise Security Manager- Intel Security como software licenciados. Estos softwares mencionados anteriormente fueron las posibles soluciones que decidió el autor del informe debido a las necesidades que tenía y la complementación que estos le daban, el cual se lleva a cabo junto con otros dos más para demostrar la efectividad que puede tener un SIEM Open Source como uno licenciado.

Finalmente el autor concluye con la siguiente frase: "Se recomienda que al no contar con recursos económicos al momento para realizar una inversión de este tipo debido a la situación actual que vive el país, se utilice la versión gratuita de USM el cual es OSSIM, el mismo que difiere de su versión comercial en lo siguiente: el soporte en OSSIM viene dado por una comunidad en base a foros y vivencias propias de los usuarios, retención de logs solo para los eventos SIEM, 3 niveles de reportes y el desarrollo del número de reglas de correlación son realizadas por la comunidad y no son tantas como USM. A pesar de esto como la infraestructura del MINTEL no es grande se concluye que OSSIM puede acoplarse y prestará gran ayuda para detectar amenazas, ataques, vulnerabilidades y con esto alertar

cuando suceda algún evento de seguridad" (Boada, 2016). Esto nos indica que fue un caso exitoso con la implementación de un SIEM utilizando Alienvault OSSIM.

3. METODOLOGÍA

3.1 Fase 1

La red del ITM se distribuye de la siguiente manera:

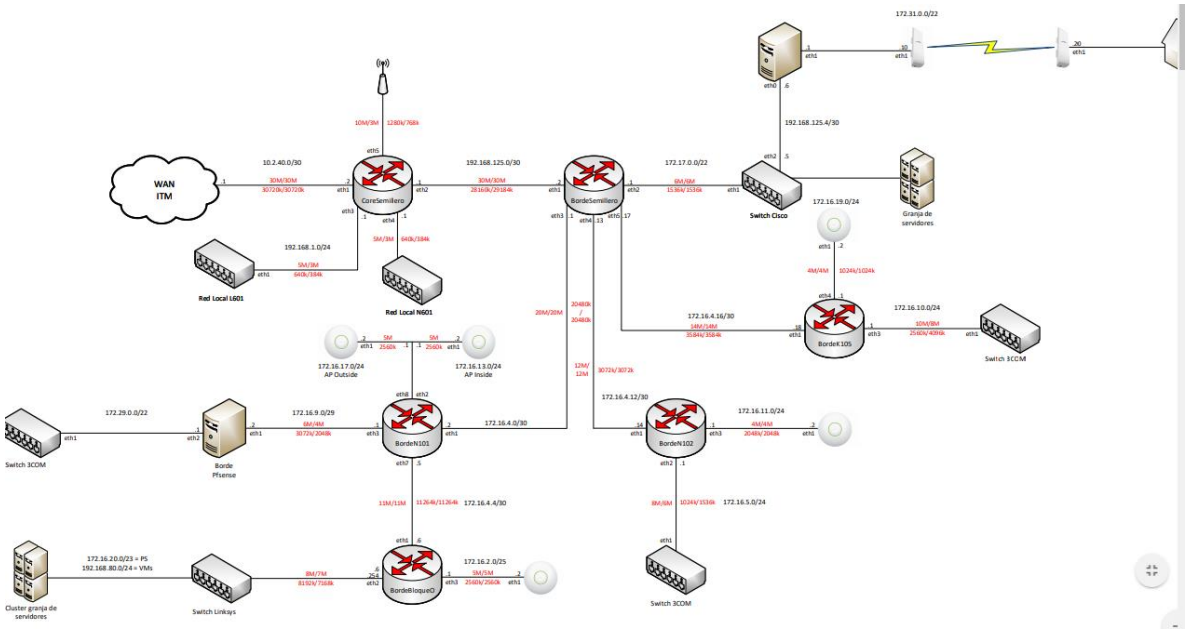


Ilustración 8.Red ITM (Elaboración propia)

Como se puede observar en la *Ilustración 8.Red ITM (Elaboración propia)* la red del ITM se compone de una serie de enrutadores (Mikrotik), los cuales son los encargados de dar servicio de internet a todos los laboratorios y parte de las redes Wi-fi. Pero para el caso de este proyecto nada más nos centraremos en la siguiente parte de la red que está enfocado hacia el bloque O. El cual será monitoreado:

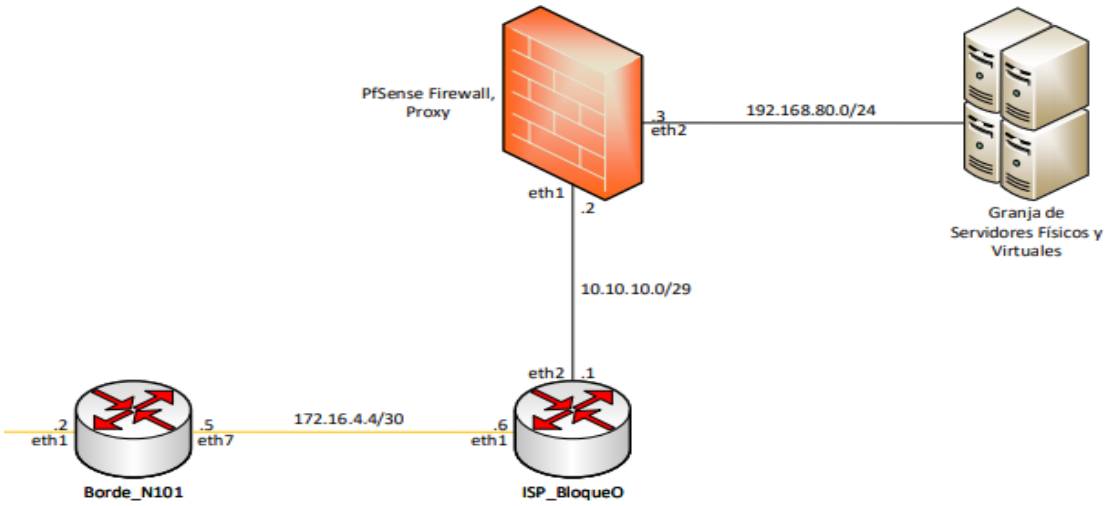


Ilustración 9.Red Bloque O (Elaboración propia)

El bloque O del Instituto Tecnológico Metropolitano está compuesto de varios laboratorios y oficinas, los cuales algunas están en proceso de crecimiento y acondicionamiento para poner en marcha con las respectivas labores. Dichos laboratorios son utilizados para clases programadas, prácticas de laboratorio independientes y lo más importante montajes para trabajos de grado de varios estudiantes.

Los laboratorios y oficinas que lo componen son: laboratorio y oficina de redes convergentes (principal), laboratorio de microelectrónica, laboratorio de biomecánica, laboratorio y oficina de sistemas, oficina de metrología.

La infraestructura principal del bloque O tanto física como lógica, está alojada en el salón de redes convergentes. Cuenta con dispositivos de red de alto costo y alto rendimiento, servidores físicos que proveen servicios y es donde están alojados muchos trabajos de grado que ya han sido presentados por estudiantes y también algunos que están en ejecución. Por este motivo, el presente trabajo de grado se encuentra enfocado hacia dicho laboratorio por la gran importancia que representa y también el flujo de información que maneja.

Ahora bien, en la siguiente ilustración se mostrará cómo está distribuida la infraestructura física/virtual en el salón de redes convergentes:

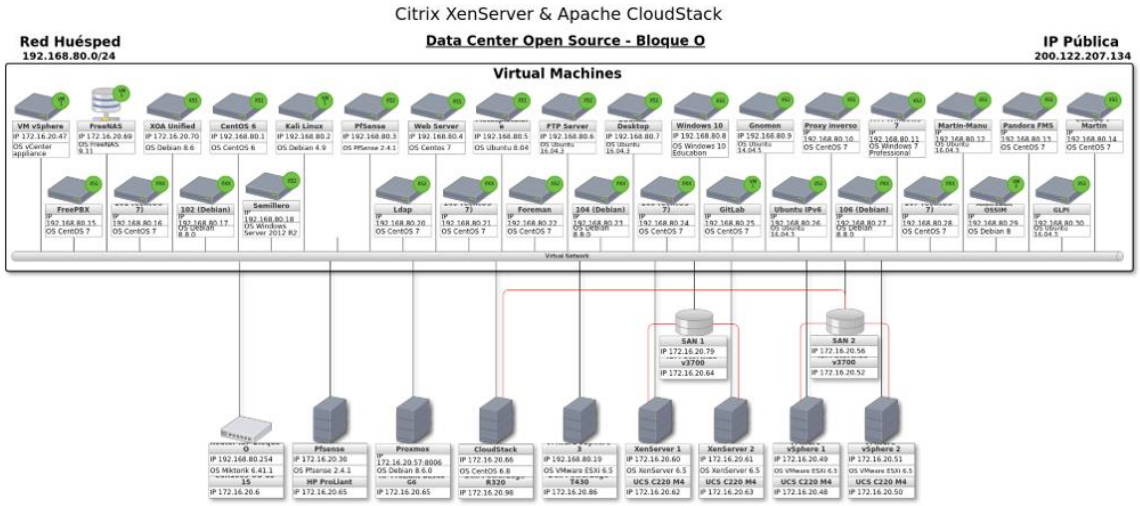


Ilustración 10.Infraestructura física/virtual Bloque O (Elaboración propia)

En la *Ilustración 10.Infraestructura física/virtual Bloque O (Elaboración propia)* el rectángulo ubicado en la parte superior representa las maquina virtuales, y en la parte de abajo son los servidores físicos que es donde se encuentran los Hipervisores (Plataforma que sirve para controlar la virtualización de diversos SO al mismo tiempo).

Teniendo una visión más clara de cómo está distribuida la red de datos que se encuentra en el bloque O, se procede a realizar el levantamiento de los activos que se encuentran alojados en dicho bloque. Este levantamiento de activos corresponde a los activos que se encuentran virtualizados y los que están físicamente operando. Además, también se especificará la ubicación, servicio prestado, cantidad y un aspecto importante, la posible amenaza que pueda tener según el servicio que presta.

Tabla 4.Levantamiento de activos físicos bloque O (Elaboración propia)

LEVANTAMIENTO DE ACTIVOS FISICOS BLOQUE O					
UBICACIÓN	**TIPO DE ACTIVO**	**FISICO/ VIRTUAL**	**CANTIDAD**	**SERVICIO PRESTADO**	**POSIBLES ATAQUES INFORMATICOS**
Oficina #1 (Laboratorio de rede convergente)	Computadores	FISICO	3	Son usados para el desempeño de las labores de cada laboratorista	ingeniería social, ingeniería social inversa, monitorización, autenticación, trashing, shoulder surfing, decoy (señuelos), scanning (búsqueda), snooping-downloading, snooping-looping, denegación de servicio, jamming o flooding, tampering o data diddling, ransomware, correos electrónicos, eavesdropping (Interceptación pasiva), snooping, saturación de servidores web y spoofing
	Teléfono IP	FISICO	1	Comunicación con las demás áreas de la universidad	Vishing, IP Spoofing, ARP Spoofing, TCP Spoofing,DoS, llamada fantasma.
Oficina #2 (Sistemas de información)	Computadores	FISICO	3	Son usados para el desempeño de la labores de cada laboratorista	ingeniería social, ingeniería social inversa, monitorización, autenticación, trashing, shoulder surfing, decoy (señuelos), scanning (búsqueda), snooping-downloading, snooping-looping, denegación de servicio, jamming o flooding, tampering o data diddling, ransomware, correos electrónicos, eavesdropping (Interceptación pasiva), snooping, saturación de servidores web y spoofing
	Teléfono IP	FISICO	1	Comunicación con las demás áreas de la universidad	Vishing, IP Spoofing, ARP Spoofing, TCP Spoofing, DoS, llamada fantasma.
Oficina #3 (Metrología)	Computadores	FISICO	3	Son usados para el desempeño de la labores de cada laboratorista	ingeniería social, ingeniería social inversa, monitorización, autenticación, trashing, shoulder surfing, decoy (señuelos), scanning (búsqueda), snooping-downloading, snooping-looping, denegación de servicio, jamming o flooding, tampering o data diddling, ransomware, correos electrónicos, eavesdropping (Interceptación pasiva), snooping, saturación de servidores web y spoofing

	Teléfono IP	FISICO	1	Comunicación con las demás áreas de la universidad	Vishing, IP Spoofing, ARP Spoofing, TCP Spoofing, DoS, llamada fantasma.
Laboratorio de biomecánica	Computadores	FISICO	2	Son usados para el desarrollo del material del curso de los estudiantes, ya sea en clase presencial o en trabajo independiente	ingeniería social, ingeniería social inversa, monitorización, autenticación, trashing, shoulder surfing, decoy (señuelos), scanning (búsqueda), snooping-downloading, snooping-looping, denegación de servicio, jamming o flooding, tampering o data diddling, ransomware, correos electrónicos, eavesdropping (Interceptación pasiva), snooping, saturación de servidores web y spoofing
	Switch	FISICO	1	Es un dispositivo usado para la conexión de las cámaras de las practicas del laboratorio	CAM table overflow, Media Access Control (MAC) addressspoofing, DHCP starvation, VLAN hopping, manipulaciones en Spanning-TreeProtocol (STP), saturación de direcciones MAC o ataques de flooding de MAC, CDP, contraseña de fuerza bruta, denegación de servicio (DoS).
Laboratorio de microelectrónica	Computadores	FISICO	14	Son usados para el desarrollo del material del curso de los estudiantes, ya sea en clase presencial o en trabajo independiente	ingeniería social, ingeniería social inversa, monitorización, autenticación, trashing, shoulder surfing, decoy (señuelos), scanning (búsqueda), snooping-downloading, snooping-looping, denegación de servicio, jamming o flooding, tampering o data diddling, ransomware, correos electrónicos, eavesdropping (Interceptación pasiva), snooping, saturacion de servidores web y spoofing
	Router Wifi	FISICO	1	Es el que se encarga de proveer internet a los estudiantes mediante la red wifi Microelectrónica	Ataques chop chop, café late, por diccionario o fuerza bruta, clave WPS, denegación de servicio (DoS), WPA-PSK, implantación de malware, MiM (Men in the Middle), sniffer, hostpots falsos, clave de reinstalación y puntos de acceso falsos

Laboratorio de redes convergentes	Portátiles	FISICO	11	Son usados para el desarrollo del material del curso de los estudiantes, ya sea en clase presencial o en trabajo independiente	ingeniería social, ingeniería social inversa, monitorización, autenticación, trashing, shoulder surfing, decoy (señuelos), scanning (búsqueda), snooping-downloading, snooping-looping, denegación de servicio, jamming o flooding, tampering o data diddling, ransomware, correos electrónicos, eavesdropping (Interceptación pasiva), snooping, saturación de servidores web y spoofing
	Router Mikrotik	FISICO	1	Cumple la función de router de borde para darle salida de internet a los demás equipos conectados a la red cableada	Redirección de DNS, ARP Spoofing, negación de servicio, ataques autenticación, inundación de NTP, cambio de rutas, IP Spoofing, ataque smurf, código malicioso, teardrop.
	Router ASA	FISICO	2	Actualmente no se encuentran en funcionamiento ya que son usados para las prácticas de laboratorio	Redirección de DNS, ARP Spoofing, negación de servicio, ataques autenticación, inundación de NTP, cambio de rutas, IP Spoofing, ataque smurf, código malicioso, teardrop.
	Router 2901|	FISICO	6	Actualmente no se encuentran en funcionamiento ya que son usados para las prácticas de laboratorio	Redirección de DNS, ARP Spoofing, negación de servicio, ataques autenticación, inundación de NTP, cambio de rutas, IP Spoofing, ataque smurf, código malicioso, teardrop.
	Router Voz IP	FISICO	1	Actualmente no se encuentran en funcionamiento ya que son usados para las prácticas de laboratorio	Redirección de DNS, ARP Spoofing, negación de servicio, ataques autenticación, inundación de NTP, cambio de rutas, IP Spoofing, ataque smurf, código malicioso, teardrop.

	Switch Linksys	FISICO	1	Es usado para interconectar el datacenter	CAM table overflow, Media Access Control (MAC) addressspoofing, DHCP starvation, VLAN hopping, manipulaciones en Spanning-TreeProtocol (STP), saturación de direcciones MAC o ataques de flooding de MAC, CDP, contraseña de fuerza bruta, denegación de servicio (DoS).
	Switchs	FISICO	10	Actualmente no se encuentran en funcionamiento ya que son usados para las prácticas de laboratorio	CAM tableoverflow, Media Access Control (MAC) addressspoofing, DHCP starvation, VLAN hopping, manipulaciones en Spanning-TreeProtocol (STP), saturación de direcciones MAC o ataques de flooding de MAC, CDP, contraseña de fuerza bruta, denegación de servicio (DoS).
	Servidores Cisco UCS	FISICO	2	Son usados para prestar un ambiente de virtualización con el sistema ESXi5 de VMware	IP spoofing, ataques a nivel de aplicación, denegación de servicio, denegación de servicio distribuida, pingflood, smurf, synflood, inyección de SQL o inyección de código, código de fuente pobre, fuerza bruta, cross site scripting, ping de la muerte, escaneo de puertos, envenenamiento de cache DNS, ACK flood, FTP Bounce, TCP sesión Hijacking, MiM (Men in the Middle), OS finger printing, keyloggers, LOKI, secuencia TCP, phishing, división de respuesta HTTP y envenenamiento de cookies
	Servidores Cisco UCS	FISICO	2	Son usados para prestar un ambiente de virtualización con el sistema Citrix XenServer basado en Unix	IP spoofing, ataques a nivel de aplicación, denegación de servicio, denegación de servicio distribuida, pingflood, smurf, synflood, inyección de SQL o inyección de código, código de fuente pobre, fuerza bruta, cross site scripting, ping de la muerte, escaneo de puertos, envenenamiento de cache DNS, ACK flood, FTP Bounce, TCP sesión Hijacking, MiM (Men in the Middle), OS finger printing, keyloggers, LOKI, secuencia TCP, phishing, división de respuesta HTTP y envenenamiento de cookies

	Servidores HP	FISICO	2	Tiene alojado Vmware Free. Actualmente no se encuentra en uso	IP spoofing, ataques a nivel de aplicación, denegación de servicio, denegación de servicio distribuida, pingflood, smurf, synflood, inyección de SQL o inyección de código, código de fuente pobre, fuerza bruta, cross site scripting, ping de la muerte, escaneo de puertos, envenenamiento de cache DNS, ACK flood, FTP Bounce, TCP sesión Hijacking, MiM (Men in the Middle), OS finger printing, keyloggers, LOKI, secuencia TCP, phishing, división de respuesta HTTP y envenenamiento de cookies
	Servidores DELL	FISICO	2	Uno de ellos es usado para alojar la página de matemáticas del ITM y el otro es usado para un ambiente de virtualización de Microsoft	IP spoofing, ataques a nivel de aplicación, denegación de servicio, denegación de servicio distribuida, pingflood, smurf, synflood, inyección de SQL o inyección de código, código de fuente pobre, fuerza bruta, cross site scripting, ping de la muerte, escaneo de puertos, envenenamiento de cache DNS, ACK flood, FTP Bounce, TCP sesión Hijacking, MiM (Men in the Middle), OS finger printing, keyloggers, LOKI, secuencia TCP, phishing, división de respuesta HTTP y envenenamiento de cookies
	Storewize (SAN)	FISICO	2	Es un servicio de almacenamiento que se presta para los servidores que prestan un ambiente de virtualización (ESXi5 y Citrix XenServer)	MiM (Men in the Middle)
	Cámara	FISICO	1	Monitoreo del laboratorio	MiM (Man in the Middle)
	Acces Point Ubiquiti	FISICO	1	Es el que se encarga de proveer internet a los estudiantes mediante la red wifi SemilleroTeleco	Ataques chop chop, café late, por diccionario o fuerza bruta, clave WPS, denegación de servicio (DoS), WPA-PSK, implantación de malware, MiM (Men in the Middle), sniffer, hostpots falsos, clave de reinstalación y puntos de acceso falsos

	Acces Point Cisco	FISICO	1	Actualmente no se encuentran en funcionamiento.	Ataques chop chop, café late, por diccionario o fuerza bruta, clave WPS, denegación de servicio (DoS), WPA-PSK, implantación de malware, MiM (Men in the Middle), sniffer, hostpots falsos, clave de reinstalación y puntos de acceso falsos
Laboratorio de sistemas de información	Switch	FISICO	1	Es usado proveer el servicio de internet a la red cableada de dicho laboratorio	CAM table overflow, Media Access Control (MAC) addressspoofing, DHCP starvation, VLAN hopping, manipulaciones en Spanning-TreeProtocol (STP), saturación de direcciones MAC o ataques de flooding de MAC, CDP, contraseña de fuerza bruta, denegación de servicio (DoS).
	Computadores	FISICO	22	Son usados para el desarrollo del material del curso de los estudiantes, ya sea en clase presencial o en trabajo independiente	ingeniería social, ingeniería social inversa, monitorización, autenticación, trashing, shoulder surfing, decoy (señuelos), scanning (búsqueda), snooping-downloading, snooping-looping, denegación de servicio, jamming o flooding, tampering o data diddling, ransomware, correos electrónicos, eavesdropping (Interceptación pasiva), snooping, saturación de servidores web y spoofing
	Macbook pro	FISICO	1	Es el equipo utilizado por el docente para las clases programadas	ingeniería social, ingeniería social inversa, monitorización, autenticación, trashing, shoulder surfing, decoy (señuelos), scanning (búsqueda), snooping-downloading, snooping-looping, denegación de servicio, jamming o flooding, tampering o data diddling, ransomware, correos electrónicos, eavesdropping (Interceptación pasiva), snooping, saturación de servidores web y spoofing
	Portátiles	FISICO	8	Son usados para el desarrollo del material del curso de los estudiantes, ya sea en clase presencial o en trabajo independiente	ingeniería social, ingeniería social inversa, monitorización, autenticación, trashing, shoulder surfing, decoy (señuelos), scanning (búsqueda), snooping-downloading, snooping-looping, denegación de servicio, jamming o flooding, tampering o data diddling, ransomware, correos electrónicos, eavesdropping (Interceptación pasiva), snooping, saturación de servidores web y spoofing

La tabla que se presenta a continuación describe los dispositivos que se encuentran virtualizados.

Tabla 5. Levantamiento de activos virtualizados bloque O (Elaboración propia)

LEVANTAMIENTO DE ACTIVOS VIRTUALIZADOS BLOQUE O					
Arquitectura Virtual	Free NAS	VIRTUAL	1	VM para alojamiento de ISOs y demás archivos	Ataque de clave compartida, DoS por la red, reproducción RTP, malware, Keylogger, App, IP spoofing, ataques a nivel de aplicación, denegación de servicio, denegación de servicio distribuida, pingflood, synflood, inyección de SQL o inyección de código, código de fuente pobre, fuerza bruta, cross site scripting, ping de la muerte, escaneo de puertos, envenenamiento de cache DNS, ACK flood, TCP sesión Hijacking, MiM (Men in the Middle), keyloggers, LOKI, secuencia TCP, phishing
	Xen Orchestra Web	VIRTUAL	1	VM para administrar el hipervisor XenServer	
	(LAN) Pfsense-Pfsense 2.3.4	VIRTUAL	1	VM de trabajo de grado de Firewall	
	Ubuntu Desktop 16.04.3	VIRTUAL	1	Ubuntu Desktop para administración	
	Pandora FMS - CentOS 7	VIRTUAL	1	VM para monitoreo de toda la infraestructura	
	SAN1 XenServer-IBM Storwize v3700	VIRTUAL	1	Almacenamiento de todas las máquinas virtuales en la red	
	SAN2 Vmware-IBM Storwize v3700	VIRTUAL	1	Almacenamiento de todas las máquinas virtuales en la red	
	Proxmox VE-Ubuntu 16.04	VIRTUAL	1	Servidor físico donde se encuentra instalado Proxmox VE	
	CloudStack web	VIRTUAL	1	Servidor para propósitos de computación en la nube	
	HyperV-HyperV Server 2012 R2	VIRTUAL	1	Hypervisor Windows	
	XenServer 1-Citrix XenServer	VIRTUAL	1	Servidor físico donde se encuentra instalado XenServer	
	XenServer 1-Citrix XenServer	VIRTUAL	1	Servidor físico donde se encuentra instalado XenServer	
	VMware vSphere 1-VMware ESXi 6.5	VIRTUAL	1	Servidor físico donde se encuentra instalado Vmware vSphere	
	VMware vSphere 2-VMware ESXi 6.5	VIRTUAL	1	Servidor físico donde se encuentra instalado Vmware vSphere	

	Ubuntu Server (FTP Server)	VIRTUAL	1	Es un servidor Linux FTP, por lo tanto, se deja el puerto 22 abierto (Gestión), adicionalmente tiene un servicio FTP en donde debe tener dos puertos abiertos el puerto 21 que es el puerto de control y el 20 que es el puerto de datos (Este abre cuando se está recibiendo información, si el servicio FTP es activo. Si el servicio está configurado como pasivo se debe conocer el rango de puertos dinámicos, debido a que cuando se realiza la conexión con el servidor se define aleatoriamente un puerto para datos). Los demás puertos se deben cerrar ya que no corresponde al rol del servidor.	
	CentOS 7 (Daniel Jimenez)	Virtual	1	Es un servidor Linux, por lo tanto se deja el puerto 22 abierto (Gestión)	
	Load Balancer	Virtual	1	Es un servidor Linux, por lo tanto se deja el puerto 22 abierto (Gestión)	
	VMware vSphere 1	Virtual	1	Es un servicio hipervisor y solo se necesita el de monitoreo que sería el puerto 161, el resto se cierra debido a que es un hipervisor y de los puertos que tiene abierto solo se ve necesario el 161.	

	VMware vSphere 2	Virtual	1	Es un servicio hipervisor y solo se necesita el de monitoreo que sería el puerto 161, el resto se cierra debido a que es un hipervisor y de los puertos que tiene abierto solo se ve necesario el 161.	
	Proxmox	Virtual	1	Es un servidor hipervisor, y los puertos que debe tener abiertos no aparecieron en el escaneo, por lo tanto, se cierra estos puertos ya que no se conoce su funcionalidad. Por defecto el puerto que usa Proxmox es el 8006	
	Windows 7.3 - Windows 7 Ultimate	VIRTUAL	1	VM de pruebas	
	Windows 10.2- Windows 10 Education	VIRTUAL	1	VM de pruebas para el firewall PfSense	
	Windows 7 (ITM Windows)	VIRTUAL	1	Es un servidor Windows orientado a las VPN, por lo tanto, se deja el puerto 3389 abierto (Escritorio Remoto), el 161 por ser puerto de monitoreo del servidor se deja abierto, el 500 porque es un servicio de VPN remota y 4500 se abre debido a que es un servicio VPN. Los puertos 135, 139 y 445 se cierran debido son puertos de carpeta compartida y se cierra ya que no se tiene conocimiento de que ese servidor tenga activo ese servicio, el 7070 se cierra debido a que no se identifica que se necesita un servicio de Streaming, el 514 se cierra debido a que es un servicio donde se almacena LOG, por lo tanto este puerto no debería estar abierto ya que debe administrarse internamente, el resto se cierra	

				debido a que no se necesita de conocimiento de que hace el servidor y por qué se encuentra esos puertos abiertos. Se LLAMA Windows 7	
	Windows 7	Virtual	1	Es un servidor Windows de VPN, por lo tanto se deja el puerto 3389 abierto (Escritorio Remoto), el puerto 500 y 161 porque son de monitoreo, el resto se cierra debido no se cuenta como un servicio asociado	
	Windows 7,2	Virtual	1	Es un servidor Windows, por lo tanto se deja el puerto 3389 abierto (Escritorio Remoto), el puerto 135 y 445 son carpeta compartidas.	
	CentOS 6 “Servidor WEB”	VIRTUAL	1	Es un servidor Linux que almacena una página web, por lo tanto, se deja el puerto 22 abierto (Gestión), además de eso se encuentra un servidor web por el puerto 80 que contiene la página de Apache 2 Test Page. EXISTE	Ataque por injeccion, DDoS, fuerza bruta, Crosse Site scripting, phishing, craqueo de contraseñas, intercepción, división de respuesta HTTP, IP spoofing, ataques a nivel de aplicación, denegación de servicio, denegación de servicio distribuida, envenamiento de coockies

	CentOS 7 “Servidor WEB”	VIRTUAL	1	Es un servidor Linux que almacena una página web, por lo tanto, se deja el puerto 22 abierto (Gestión), además de eso se encuentra un servidor web por el puerto 80 que contiene la página de HTTP Web Example. EXISTE	
	Elastix 2.5 “Servidor WEB”	VIRTUAL	1	Es un servidor Linux orientado a telefonía, por lo tanto se deja el puerto 22 abierto (Gestión), además de eso se encuentra un servidor web por el puerto 80 que contiene la página de HTTP y el puerto 443 contiene la página de HTTPS, el puerto 5060 por donde funciona los teléfonos, el puerto 123 es para la sincronización de reloj entre los teléfonos y el servidor y el puerto 69 para descargar versiones a los teléfonos debido a que el servidor es un servidor de telefonía. El puerto 3306 se cierra debido a que es un puerto de base de datos, y debe ser accesible solo por el servidor, el puerto 25, 110 y 143 se cierra debido es un puerto de correos, el puerto 111 se cierra por que es para enviar comando remoto y es un puerto vulnerable, el puerto 4569 no debería estar abierto ya que es un protocolo para lanzar centrales telefónicas, el resto se cierra debido se conoce su servicio.	

	Elastix 4 “Servidor WEB”	Virtual	1	Es un servidor Linux orientado a telefonía, por lo tanto, se deja el puerto 22 abierto (Gestión), además de eso se encuentra un servidor web por el puerto 80 que contiene la página de HTTP y el puerto 443 contiene la página de HTTPS, el puerto 68 para asignaciones de direcciones IP dinámicas, el puerto 69 para descargar versiones a los teléfonos y el puerto 5060 por donde funciona los teléfonos. El puerto 25, 110, 993 y 143 se cierra debido es un puerto de correos, el puerto 2727 no está orientando a los usuarios, el puerto 4569 no debería estar abierto ya que es un protocolo para lanzar centrales telefónicas, el resto se cierra debido se conoce su servicio.	
	Apache CloudStack	Virtual	1	Encargada de coordinar de manera centralizada el aprovisionamiento automático de capacidades de cómputos y sus dependencias (almacenamiento, redes y sistemas operativos).	
	Windows Server 2012 R2 (Semillero) “Servidor WEB”	Virtual	1	Es un servidor Windows, por lo tanto se deja el puerto 3389 abierto (Escritorio Remoto), un servidor que es un controlador de dominio por lo tanto se abre los puertos asociados a un controlador de dominio y se cierran los demas	Ataque por injeccion, DDoS, fuerza bruta, Crosse Site scripting, phishing, craqueo de contraseñas, intercepción, web spoofing, Ataque de clave compartida, DoS por la red, reproducción RTP, malware, Keylogger, APP, ataque por injeccion, DDoS, fuerza bruta, Crosse Site scripting, phishing, craqueo de contraseñas, intercepción, división

					de respuesta HTTP, IP spoofing, ataques a nivel de aplicación, denegación de servicio, denegación de servicio distribuida, envenamiento de coockies

Se puede observar en las dos tablas anteriores una cantidad considerable de dispositivos, es difícil realizar (para el proyecto) una configuración de logs y correlación en todos, por lo cual se define un alcance basado en los mismos objetivos, éste se enfoca en los elementos alojados en el laboratorio de redes convergentes ya que son los que representan un nivel más elevado de vulnerabilidad en cuanto al servicio que prestan y son de vital importancia para el funcionamiento de la red y demás trabajos de grado que están pendientes por culminar o que también estén operando en el momento.

De acuerdo a lo anterior surge una pregunta muy importante: ¿Cómo saber que dispositivos se escogen?, ya que dependiendo de esta selección se hará el monitoreo respectivo a un grupo de equipos que son los más significativos y además de eso representan el encabezado inicial de la red de datos o también considerado como el primer filtro de lo que puede representar el inicio de un ataque informático.

Para dar respuesta a la pregunta, se ha realizado un mapa de riesgos y de acuerdo al posible impacto obtenido, se han seleccionado los elementos tecnológicos más representativos y/o que están en alto riesgo de un problema de seguridad. Un riesgo es la posibilidad que una amenaza de seguridad se ejecute sobre un activo y genere un impacto negativo sobre dicho sistema.

El mapa de riesgos es un procedimiento articulado y secuencial que permite, a través de una herramienta, calculando su magnitud y estableciendo estrategias para el manejo de dichos riesgos. (Manuel Rodriguez Lopez, 2013)

Una vez que se logran identificar los riesgos, éstos deben calcularse acorde a la probabilidad de ocurrencia y al impacto que pueden generar, con ello, se ve en la necesidad de tomar acciones para poder medirlos y darles una prioridad.

La fórmula usada para calcular el valor del riesgo fue la siguiente:

$$Riesgo = Probabilidad * Impacto$$

El proceso de análisis de riesgos realizado fue el siguiente:

1) Levantamiento de activos en el bloque O, laboratorio de redes convergentes.
2) Obtención de las posibles amenazas a los sistemas
3) Definición de las tablas de probabilidad e impacto
4) Creación de los escenarios de riesgos.
5) Calificar los riesgos y obtener el mapa respectivo.

A continuación, en la siguiente tabla se muestra cómo se dividen los niveles de importancia:

Tabla 6.Niveles de importancia básicos (Manuel Rodriguez Lopez, 2013)

Nivel de importancia	Descripción
Alta	Puede afectar a un número n de procesos o productos que son gestionados por un área y también pueden representar una pérdida económica sustancial.
Medio	Puede afectar a un número de procesos o productos que son gestionados por un área y también pueden representar una pérdida económica significativa
Baja	Puede afectar a un número n reducido de procesos o productos que son gestionados por un área y también pueden representar una pérdida económica moderada

Adicionalmente a este nivel de importancia se debe tener en cuanta de la probabilidad con la que pueda ocurrir como se muestra a continuación:

Tabla 7. Nivel de probabilidad (Manuel Rodriguez Lopez, 2013)

Nivel de probabilidad	Descripción	Frecuencia

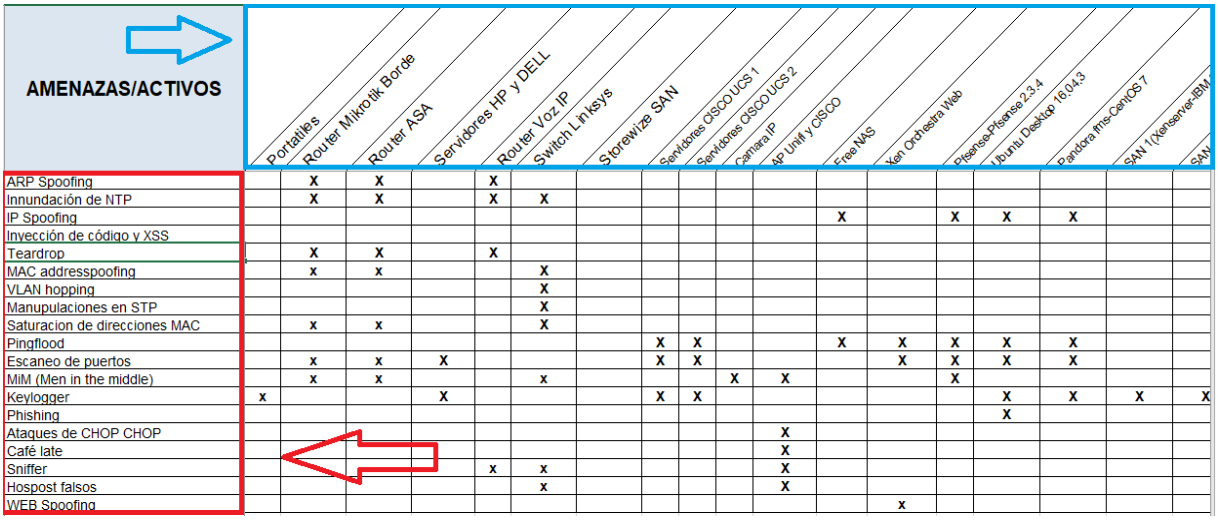
Alta	Probablemente ocurrirá en la mayoría de las circunstancias.	1 vez al mes
Medio	Puede ocurrir en algún momento.	1 vez al trimestre
Baja	Podría ocurrir en pocas circunstancias.	1 vez al trimestre

Una vez calificados los escenarios de riesgos, se obtiene el respectivo mapa de riesgos (ilustración 11). El color rojo en un mapa de riesgos representa un riesgo alto, el color amarillo representa un riesgo medio y el verde un riesgo bajo. Teniendo estos conceptos claros podemos sintetizar las dos ideas anteriores plasmadas en las tablas de la siguiente manera:

Probabilidad	valor	Impacto		
		1	2	3
Posible	3			
Improbable	2			
Raro	1			

Ilustración 11.Ejemplo de mapa de riesgos. Elaboración propia con base en (Manuel Rodriguez Lopez, 2013)

Haciendo un análisis crítico se nota que la mayoría de los servidores y máquinas virtuales que están virtualizados se encontraban alojados en los servidores físicos que contienen Hipervisores para su administración, debido a esto, se concluye monitorear solo los dispositivos físicos.



AMENAZAS/ACTIVOS	Portatiles	Router Mikrotik Borde	Router ASA	Servidores HP y DELL	Router Voz IP	Switch Linksys	Storewize SAN	Servidores CISCO UCS 1	Servidores CISCO UCS 2	Camara IP	AP Unifi y CISCO	Free NAS	Xen Orchestra Web	Ptsense-Ptsense 2.3.4	Ubuntu Desktop 16.04.3	Pandora fms-CentOS 7	SAN 1(Xenserver-IBM	SAN
ARP Spoofing		X	X		X													
Innundación de NTP		X	X		X	X												
IP Spoofing												X		X	X	X		
Invección de código y XSS																		
Teardrop		X	X		X													
MAC addresspoofing		x	x			X												
VLAN hopping						X												
Manupulaciones en STP						X												
Saturacion de direcciones MAC		x	x			X												
Pingflood								X	X			X	X	X	X	X		
Escaneo de puertos		x	x	X				X	X				X	X	X	X		
MiM (Men in the middle)		x	x			x				X	X			X				
Keylogger	x			X				X	X						X	X	X	X
Phishing															X			
Ataques de CHOP CHOP											X							
Café late											X							
Sniffer					x	x					X							
Hospost falsos						x					X							
WEB Spoofing													x					

Ilustración 12. Extracto Activos físico vs. posibles ataques según los servicios (Elaboración propia)

Partiendo desde lo concluido anteriormente, en la *Ilustración 12. Extracto Activos físico vs. posibles ataques según los servicios (*Elaboración propia), es un extracto de la lista, para lo cual, se cotejaron los datos mirando los posibles ataques que pueden ocurrir ubicados en el recuadro señalado con rojo. Estos tipos de ataques se confrontaron según el dispositivo y el servicio que se ofrece. Estos se encuentran señalados en el recuadro azul.

Seguidamente después de plantear el escenario de riesgos anterior, se realizó el cálculo de riesgos a través de un archivo Excel creado para tal fin. Estos resultados se evidenciaron de la siguiente manera:

2	Escenario del riesgos
3	Ingenieria social -- Estudiantes y Profesores
4	DoS (Negación de servicio) -- Portatiles
5	DoS (Negación de servicio) -- Router Mikrotik Borde
6	DoS (Negación de servicio) -- Router ASA
7	DoS (Negación de servicio) -- Servidores HP y DELL
8	DoS (Negación de servicio) -- Router Voz IP
9	DoS (Negación de servicio) -- Switch Linksys
10	DoS (Negación de servicio) -- Storewize SAN
11	DoS (Negación de servicio) -- Servidores CISCO UCS 1
12	DoS (Negación de servicio) -- Servidores CISCO UCS 2
13	DoS (Negación de servicio) -- Camara IP
14	DoS (Negación de servicio) -- AP Unifi y CISCO
15	DoS (Negación de servicio) -- Free NAS
16	DoS (Negación de servicio) -- Xen Orchestra Web
17	DoS (Negación de servicio) -- Pfsense-Pfsense 2.3.4
18	DoS (Negación de servicio) -- Ubuntu Desktop 16.04.3
19	DoS (Negación de servicio) -- Pandora fms-CentOS 7
20	DoS (Negación de servicio) -- SAN 1(Xenserver-IBM Storewize)
21	DoS (Negación de servicio) -- SAN 2(Vmware-IBM Storewize)
22	DoS (Negación de servicio) -- Proxmox VE-Ubuntu 16.04
23	DoS (Negación de servicio) -- Cloudstack WEB
24	DoS (Negación de servicio) -- HyperV-Hyperv Server 2012 R2
25	DoS (Negación de servicio) -- Ubuntu Server (FTP Server)
26	DoS (Negación de servicio) -- CentOS 7(Daniel Jimenez)
27	DoS (Negación de servicio) -- Vmware vSphere

TABLAS | escenario de riesgo | Agentes | calificacion-Control | Aceptabilidad-Control

Ilustración 13. Resultado del cotejamiento de datos (Elaboración propia)

Como se puede evidenciar los datos que se cotejaron anteriormente, gracias a la programación del archivo de Excel aparecen de forma más ordenada para una visualización mejor.

Seguidamente se procede a hacer la calificación de controles como se muestra en la siguiente ilustración.

Calificación con Controles

ESCENARIO	PROBABILIDAD		IMPACTO OPERACIÓN		Riesgo P*Impacto Cliente Mercado
Ingenieria social -- Estudiantes y Profesores	baja	1	Bajo	1	1
DoS (Negación de servicio) -- Portatiles	baja	1	Bajo	1	1
DoS (Negación de servicio) -- Router Mikrotik Borde	media	2	alto	3	6
DoS (Negación de servicio) -- Router ASA	media	2	medio	2	4
DoS (Negación de servicio) -- Servidores HP y DELL	media	2	medio	2	4
DoS (Negación de servicio) -- Router Voz IP	media	2	medio	2	4
DoS (Negación de servicio) -- Switch Linksys	media	2	alto	3	6
DoS (Negación de servicio) -- Storewize SAN	media	2	medio	2	4
DoS (Negación de servicio) -- Servidores CISCO UCS 1	media	2	alto	3	6
DoS (Negación de servicio) -- Servidores CISCO UCS 2	media	2	alto	3	6
DoS (Negación de servicio) -- Camara IP	media	2	medio	2	4
DoS (Negación de servicio) -- AP Unifi y CISCO	media	2	medio	2	4
DoS (Negación de servicio) -- Free NAS	media	2	medio	2	4
DoS (Negación de servicio) -- Xen Orchestra Web	media	2	medio	2	4
DoS (Negación de servicio) -- Pfsense-Pfsense 2.3.4	media	2	medio	2	4
DoS (Negación de servicio) -- Ubuntu Desktop 16.04.3	media	2	Bajo	1	2
DoS (Negación de servicio) -- Pandora fms-CentOS 7	media	2	Bajo	1	2
DoS (Negación de servicio) -- SAN 1(Xenserver-IBM Storewize)	media	2	medio	2	4
DoS (Negación de servicio) -- SAN 2(Vmware-IBM Storewize)	media	2	medio	2	4
DoS (Negación de servicio) -- Proxmox VE-Ubuntu 16.04	media	2	medio	2	4
DoS (Negación de servicio) -- Cloudstack WEB	media	2	medio	2	4
DoS (Negación de servicio) -- HyperV-Hyperv Server 2012 R2	media	2	medio	2	4
DoS (Negación de servicio) -- Ubuntu Server (FTP Server)	media	2	Bajo	1	2
DoS (Negación de servicio) -- CentOS 7(Daniel Jimenez)	media	2	Bajo	1	2
DoS (Negación de servicio) -- Vmware vSphere	media	2	medio	2	4
DoS (Negación de servicio) -- Proxmox	media	2	medio	2	4
DoS (Negación de servicio) -- Windows 7.x	baja	1	Bajo	1	1
DoS (Negación de servicio) -- CentOS 6 (Servidor WEB)	baja	1	Bajo	1	1
DoS (Negación de servicio) -- GNOMON	media	2	medio	2	4
DoS (Negación de servicio) -- CentOS 7 (Servidor WEB)	baja	1	medio	2	2
DoS (Negación de servicio) -- Elastix 2.5 Servidor WEB	baja	1	medio	2	2
DoS (Negación de servicio) -- Elastix 4 WEB	baja	1	medio	2	2
DoS (Negación de servicio) -- Apache Cloudstack	media	2	medio	2	4
DoS (Negación de servicio) -- Windows Server 2012 R2- Semillero WEB	media	2	medio	2	4
Ransomware -- Portatiles	baja	1	Bajo	1	1
Ransomware -- Servidores HP y DELL	media	2	medio	2	4

Ilustración 14. Calificación de controles (Elaboración propia)

Para la calificación de la probabilidad e impacto, se tomaron referencias del mercado y experiencia del asesor. Esta etapa es de suma importancia debido a los resultados posteriores obtenidos en el mapa de riesgos (Riesgo = probabilidad * impacto).

Después de hacer la evaluación respectiva según la importancia que signifique el activo en la red se obtuvo el siguiente mapa de riesgos. Luego, se procedió a realizar la evaluación del mapa de riesgos con los dispositivos ubicados en el laboratorio de redes convergentes, tomando como entradas las diferentes amenazas identificadas.

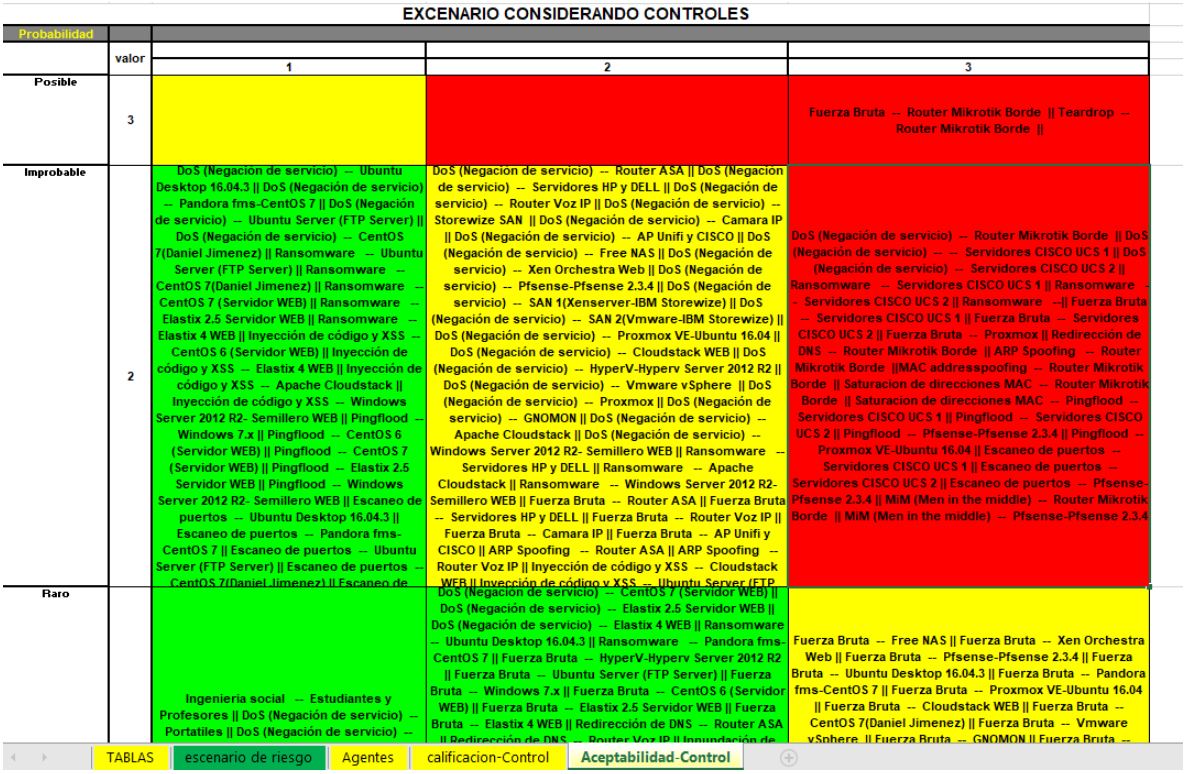


Ilustración 15. Mapa de riesgos bloque O (Elaboración propia)

Se puede observar en la *Ilustración 15. Mapa de riesgos bloque O (Elaboración propia)* se muestran los tres colores de muestro mapa de riesgos. Los planes de tratamiento de riesgos deben ser enfocados a los riesgos que están en rojo, ya que son los que representan un riesgo más alto y son a los que se les debe poner especial cuidado.

3.2 Fase 2

Según el análisis realizado en la fase 1 se toma la decisión de monitorear todos los equipos en su totalidad y no por servicios como se había acordado en la propuesta inicial. De esta manera se hace una implementación mucho más completa, haciendo que la seguridad se abarque en un gran porcentaje para uno de los dispositivos.

Dentro del levantamiento de activos, se identificó la existencia de un correlacionador de eventos básico (Alienvault OSSIM), el cual fue potencializado y mejorado con éste proyecto. Como parte de la identificación, se a revisar el estado se encuentra el SIEM, es decir que dispositivos tiene alojados en su monitoreo, que tipo de reglas de correlación tiene

configuradas, como se encuentra el estado de los sensores, características de rendimiento del servidor, tráfico de syslog en tiempo real, entre otros, dado que ésta información se usó para potenciar éste proyecto.

El SIEM puede ser implementado para la recolección de eventos de seguridad o para que dichos eventos sean enviados desde los dispositivos finales, para lo cual, es posible la configuración de agentes en dispositivos o activar protocolos como Syslog o SNMP.

3.3 Fase 3

Tomando como base el análisis anterior y considerando la necesidad propia del proyecto, se decidió montar un nuevo servidor teniendo en cuenta la configuración de los diferentes plugins asociados a los activos cuyos riesgos fueron catalogados en alto. La instalación del nuevo SIEM se detalla en el apéndice A.

Seguidamente después de que OSSIM haya terminado de instalar procedemos a hacer la configuración inicial por medio de la interfaz web, de la siguiente manera:

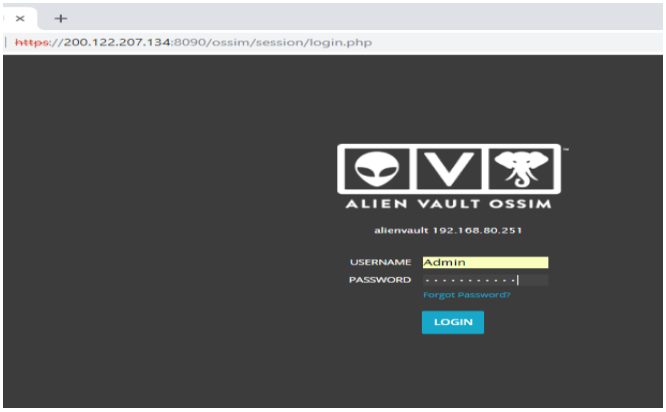


Ilustración 16. Acceso por interfaz web al nuevo servidor (Elaboración propia)

Inmediatamente que se ingresa, se encuentra la siguiente configuración

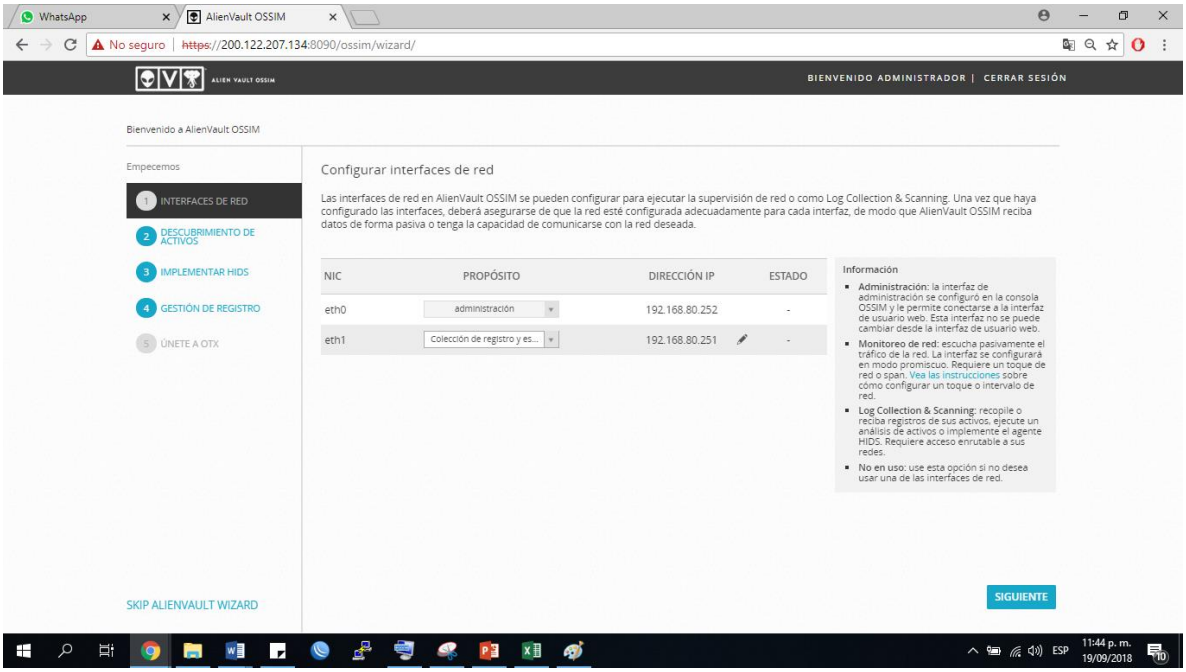


Ilustración 17. Interfaces de red nuevo servidor (Elaboración propia)

En la ilustración anterior se puede ver dos interfaces de red, la cual la eth0 está destinada para el gestionamiento del servidor, y la Eth1 es la que tiene que ser debidamente configurada en cada uno de los dispositivos para la recolección de logs, seguidamente se hacía un escaneo a la red que se va a monitorear, con ello, el sistema logra encontrar diferentes dispositivos que hacen parte de la red (descubrimiento propio).

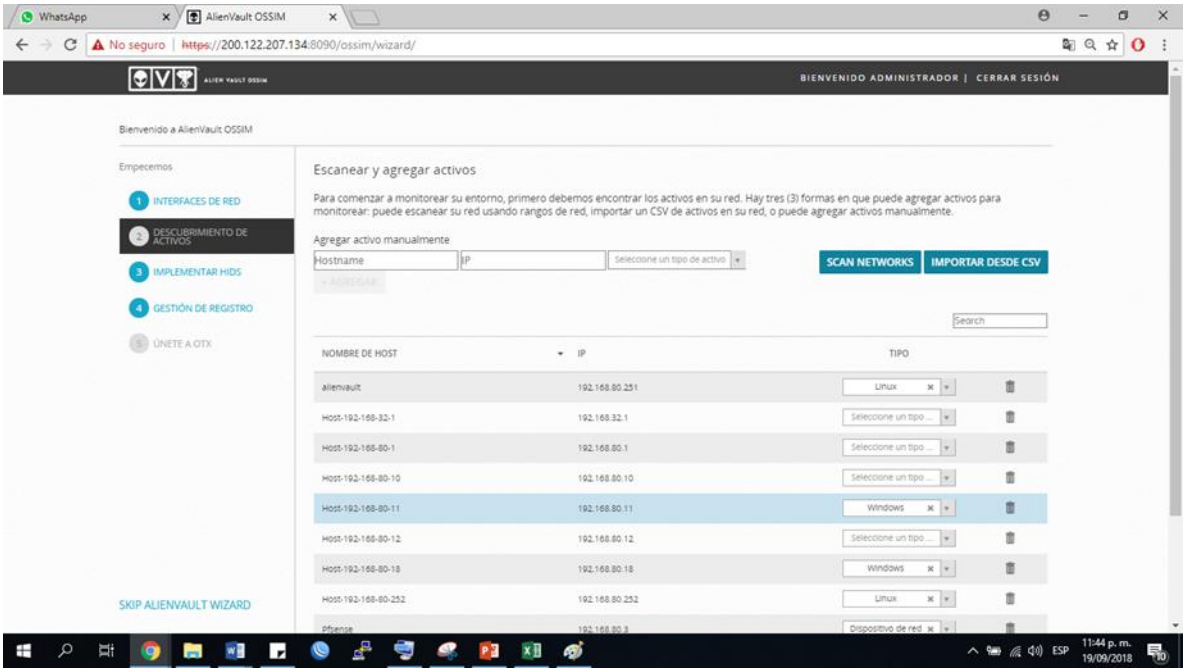


Ilustración 18. Escaneo de red (Elaboración propia)

Adicionalmente se agregaron los dispositivos restantes por monitorear manualmente que no aparecieron en el escaneo, con sus respectivas direcciones IP (suministradas por el administrador de red). Seguidamente se procedía a la configuración de los plugins.

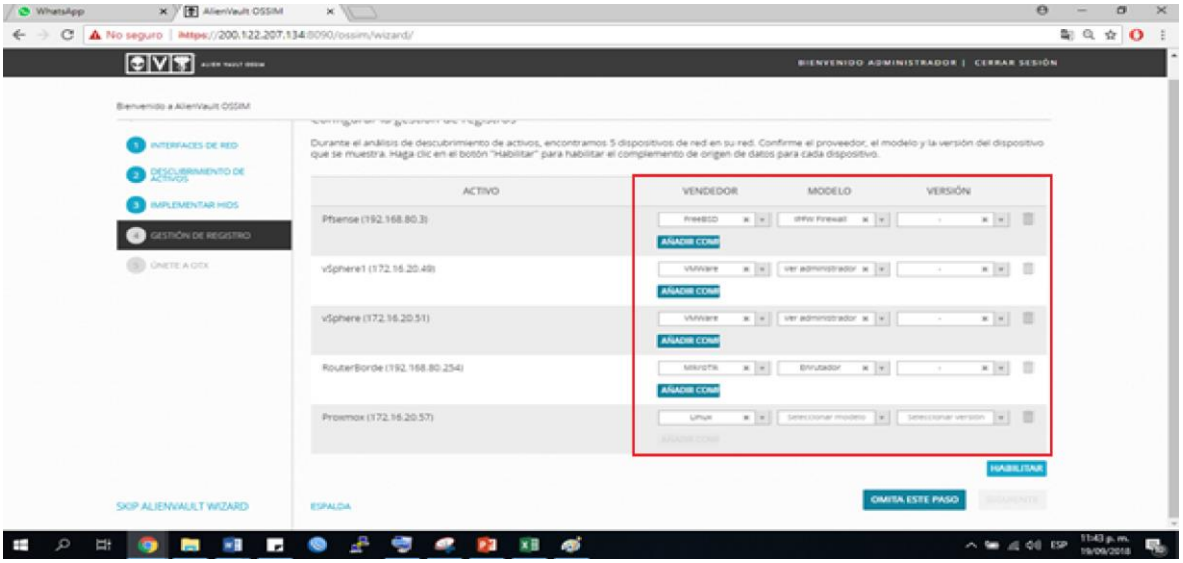


Ilustración 19. Configuración de plugins nuevo servidor (Elaboración propia)

En la *Ilustración 19. Configuración de plugins nuevo servidor (Elaboración* propia) se puede observar que se señala un recuadro rojo. En dicho recuadro es donde se tienen que poner lo plugins necesarios de acuerdo al dispositivo que se tenga. Por ejemplo, el RouterBorde, es un dispositivo de marca Mikrotik, OSSIM tiene un plugin específico para enrutadores Mikrotik, entonces lo seleccionamos. Sucesivamente se procede con cada uno de los dispositivos que se tengan para monitorear.

NOTA: Es muy importante que se tenga conocimiento acerca de los sistemas base, marcas o proveedor de cada uno de los dispositivos que se van a monitorear, ya que de esto depende la selección de los plugins.

Después de haber seleccionado los plugins, se selecciona saltar al paso siguiente y por último se finaliza. Luego de esto se tendrá gestión del dispositivo para las futuras configuraciones.

Tomando como base el mapa de riesgo se tiene que los dispositivos a ser monitoreados son los siguientes:

- Router de borde Mikrotik
  IP:192.168.80.254
- Servidor CISCO UCS 1 (Hipervisor Xenserver)
  Xenserver1: 172.16.20.60
  Xenserver2: 172.16.20.61

- Servidor CISCO UCS 2 (Hipervisor vSphere)
  vSphere1: 172.16.20.49
  vSphere2: 172.16.20.51

- Hipervisor Proxmox
  IP:172.16.20.57
- Pfsense

IP:192.168.80.3

Con el fin de darle un mejor orden y manejo, se crea un grupo de activos que serán los únicos que se van a monitorear, llamado Activos Bloque O

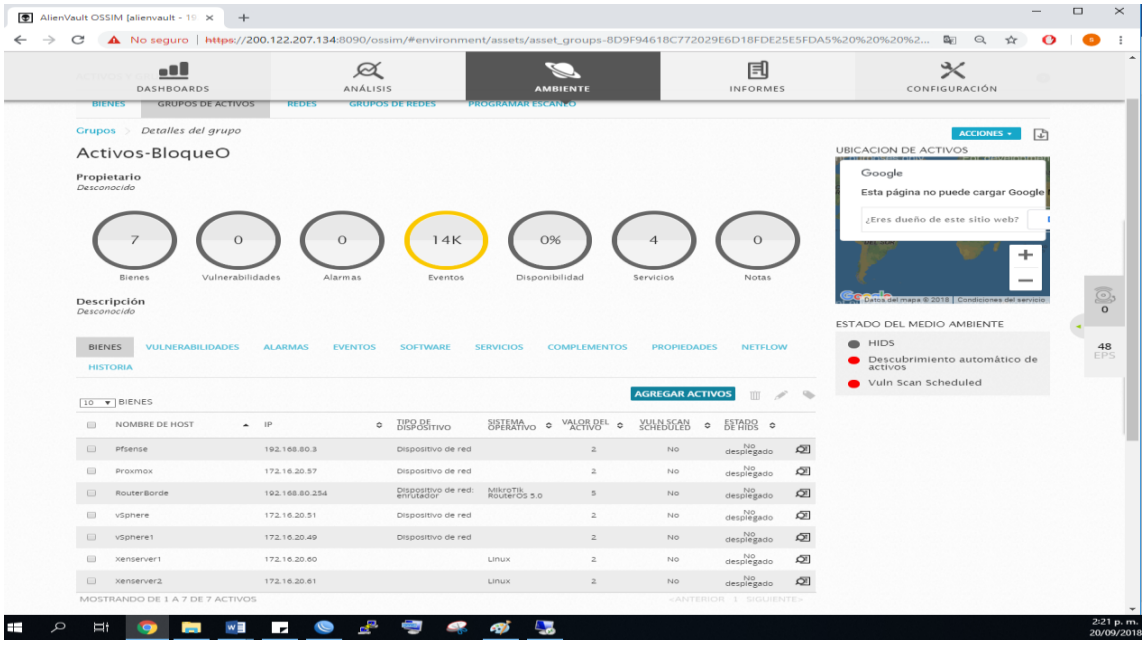


Ilustración 20. Grupo de activos Bloque O (Elaboración propia)

Luego es necesario realizar la respectiva configuración en cada uno de los dispositivos de manera que los logs que generen, sean enviados hacia el servidor OSSIM. En la siguiente ilustración 21 se muestra una visión más global a acerca de cómo funcionan los logs, en dónde una vez configurado el sistema de alertas, los dispositivos envían la información al SIEM y éste dependiendo de la regla, notifica al administrador para que tome alguna acción sobre el sistema.

Ilustración 21. Funcionamiento de logs (Network Management Software, 2018)

NOTA: la configuración de cada dispositivo se encuentra en el apéndice B

Después de hacer la respectiva configuración se observa que los equipos sí se encuentren enviando logs hacia el servidor. Este paso se puede observar de dos formas.

1) Mediante la interfaz Web

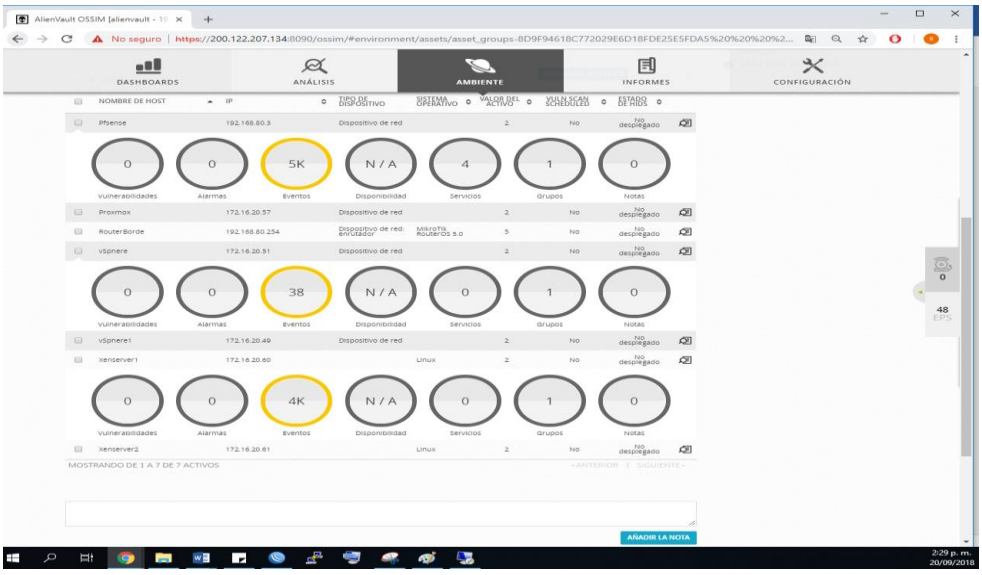


Ilustración 22. Reporte de logs mediante interfaz Web (Elaboración propia)

Como se puede observar en los círculos amarillos son eventos que reportan los dispositivos de acuerdo a la configuración que se le fue aplicada.

2) Mediante consola de comandos

Ingresamos por SSH hacia el servidor y escogemos la opción 3, Jailbreak System.

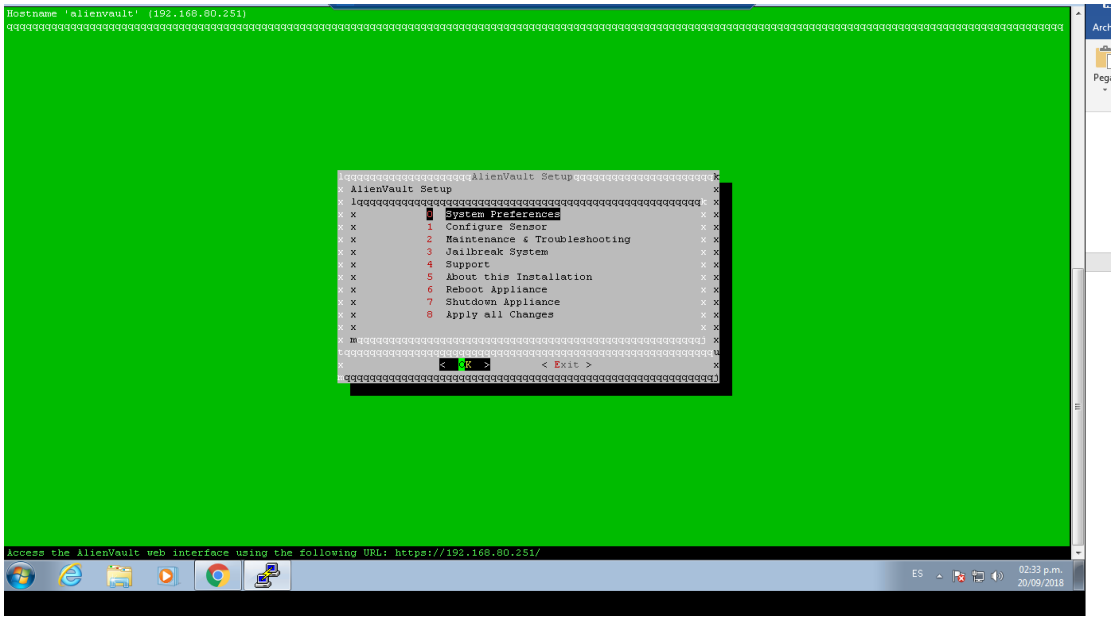


Ilustración 23. Consola de comandos Jailbreak System (Elaboración propia)

Cuando se ingresa a la consola de comandos, se escribe la siguiente línea de comandos para verificar que los logs si estén llegando al servidor. Para este caso haremos el ejemplo con la IP del router.

tcpdump | grep 192.168.80.254

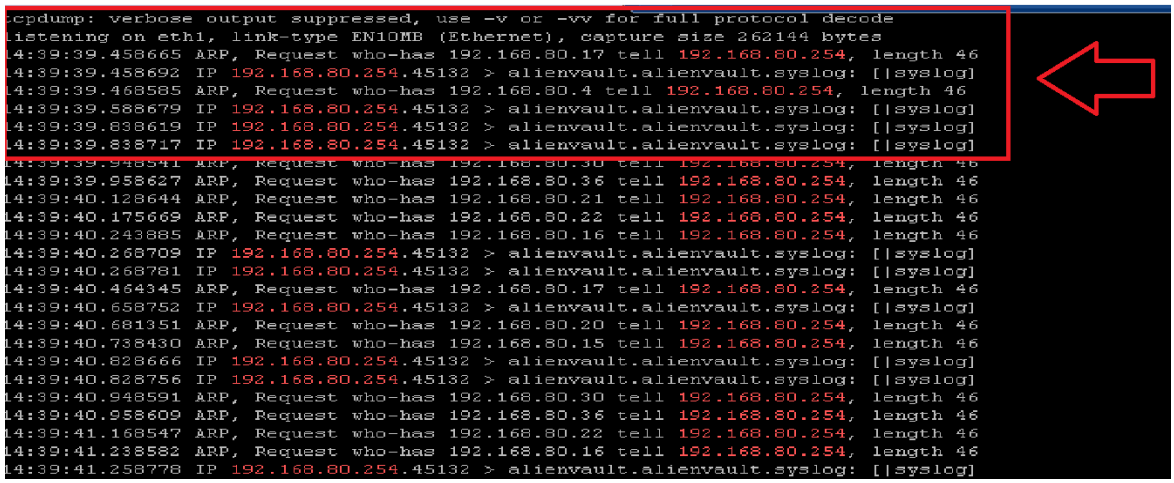


Ilustración 24. Reporte de logs mediante consola (Elaboración propia)

En el recuadro rojo de la *Ilustración 24. Reporte de logs mediante consola (Elaboración propia)*, se puede notar que el router está enviando mensajes de tipo syslog hacia el servidor Alienvault.

Después de haber corroborado esta información, hay que tener en cuenta cuales son las posibles amenazas que se presentaron en los dispositivos (tabla 8), ya que con base a esto serán diseñadas las reglas de correlación. Para esto es importante conocer cuáles son:

Tabla 8. Amenazas activos bloque O (Elaboración propia)

ACTIVOS BLOQUE O	
DISPOSITVOS	AMENAZA
Servidores Cisco UCS 1 (Xenserver)	DoS, Ransonware, fuerza bruta, pingflood, escaneo de puertos, men in the middle
Servidores Cisco UCS 2 (vSphere)	
Router Mikrotik	DoS, redirección de DNS, ARP spoofing, MAC adddresspoofing, saturación MAC, Men in the middle
Proxmox	Fuerza bruta, pingflood.
Pfsense	Pingflood, escaneo de puertos, men in the middle

Con el fin de optimizar las diferentes reglas, se hace una unificación de las amenazas, de

ésta manera se evita hacer la configuración de una regla de correlación por cada amenaza. Esta unificación se realizó de la siguiente manera:

Tabla 9. Unificación de amenazas (Elaboración propia)

UNIFICACIÓN DE AMENAZAS	
AMENAZA	**REGLA A IMPLEMENTAR**
DoS	Dos/DDoS
Pingflood	
Fuerza bruta	Fuerza bruta
Redirección DNS	Men In The Middle (MITM)
ARP Spoofing	
MAC Adresspoofing	
Saturación MAC	
Escaneo de puertos	Scanning
Inundación de NTP	NTP

Teniendo esto, se puede observar la configuración de cada una de las reglas de correlación en el Apéndice C. Las pruebas de validación de dichas reglas de correlación se mostrarán evidenciadas en la sección número 4, correspondiente a resultados y discusiones.

3.4 Fase 4

Esta fase corresponde a la documentación de las pruebas realizadas lo cual estará ubicado en la sección de resultados y discusiones. Además de las conclusiones respectivas ubicadas en la sección número 5.

4. RESULTADOS Y DISCUSIÓN

4.1 Implementación de ataques

Para la comprobación de los resultados de las reglas de correlación se hizo uso de una herramienta muy efectiva llamada Kali Linux, la cual fue diseñada con el objetivo principal de auditar y proveer seguridad a un sistema en general.

Inicialmente se hizo una consulta previa acerca de que herramientas se podían aprovechar desde el Kali Linux, para poder realizar los ataques de comprobación.

- NMAP: Por lo general es una herramienta muy usada para la identificación de los puertos que están abiertos en los dispositivos, aplicaciones que estén corriendo, tipo de sistema operativo del equipo, servicios que tengan activos, entre otros. De esta manera se pueden filtrar diversidad de ataques. (Linux, 2010)
- Hping3: Para explicar la utilidad de este comando es necesario que inicialmente de aclare cómo funciona una conexión TCP/IP, la cual funciona de la siguiente manera:

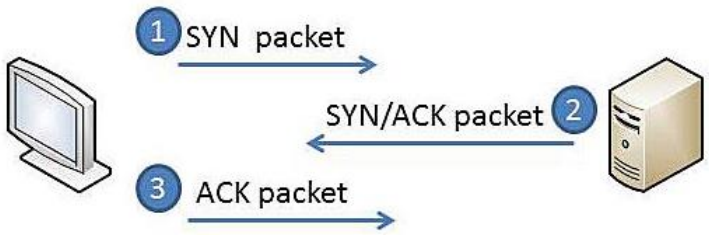


Ilustración 25. Conexión TCP (Romero, 2016)

En la *Ilustración 25. Conexión TCP (Romero,* 2016), el cliente envía un paquete tipo SYN para iniciar la comunicación con el servidor remoto, e inmediatamente el servidor le responde con un paquete SYN+ACK. Cuando el cliente recibe este paquete, le devuelve nuevamente un paquete tipo ACK. Esto es comúnmente conocido como el saludo de las tres vías.

Ahora bien, teniendo esto claro el comando *hping3* tiene la utilidad de provocar una inundación de paquetes tipo SYN, pero dejando al cliente remoto sin la espera del paquete

ACK. De esta manera se provoca una denegación de servicio ya que provoca miles de peticiones por parte del equipo remoto para poder finalizar la conexión, haciendo de esta manera que la red pueda colapsar.

- Ettercap: Es una herramienta muy utilizada por Kali Linux para realizar ataques informáticos de tipo Men In The Middle, el cual funciona como un sniffer que tiene la capacidad de escuchar y filtrar el tráfico de las comunicaciones. Por lo general esta herramienta tiene la capacidad de generar ataques tipo ARP Spoofing, el cual consiste en un envío constante de mensajes ARP (Address Resolution Protocol) falsos en una red local. (Quezada, 2014)
- Fuerza bruta: Es un ataque informático, usado como método para averiguar la contraseña de algún tipo de dispositivo con todas las combinaciones posibles.

Seguidamente los ataques usados para comprobar la eficiencia de la configuración de las reglas de configuración se notificarán a continuación junto con la comprobación de la respectiva alerta.

4.1.1 Escaneo de puertos mediante NMAP

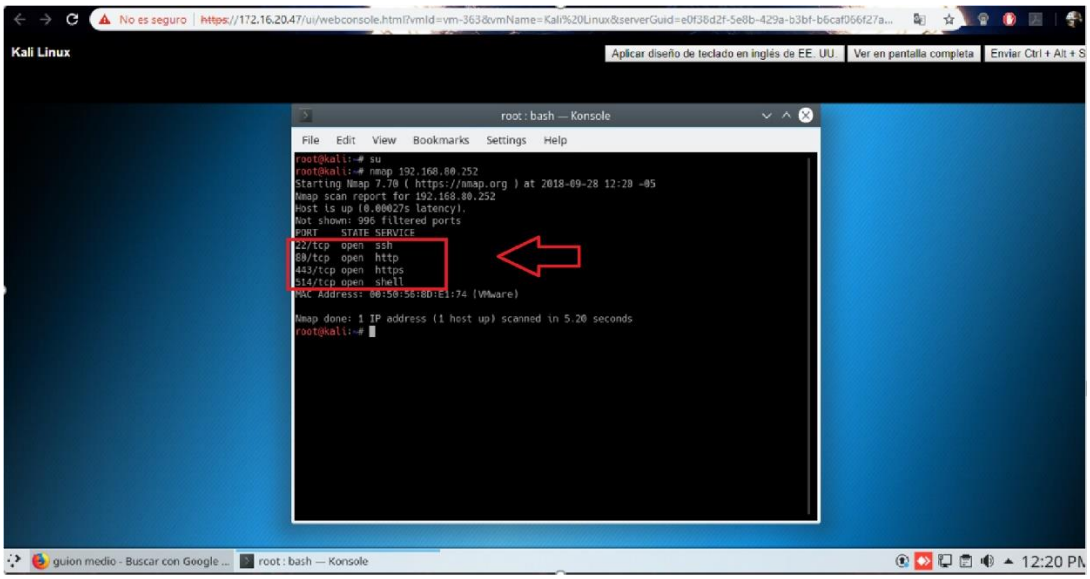


Ilustración 26. Escaneo de puertos Alienvault (Elaboración propia)

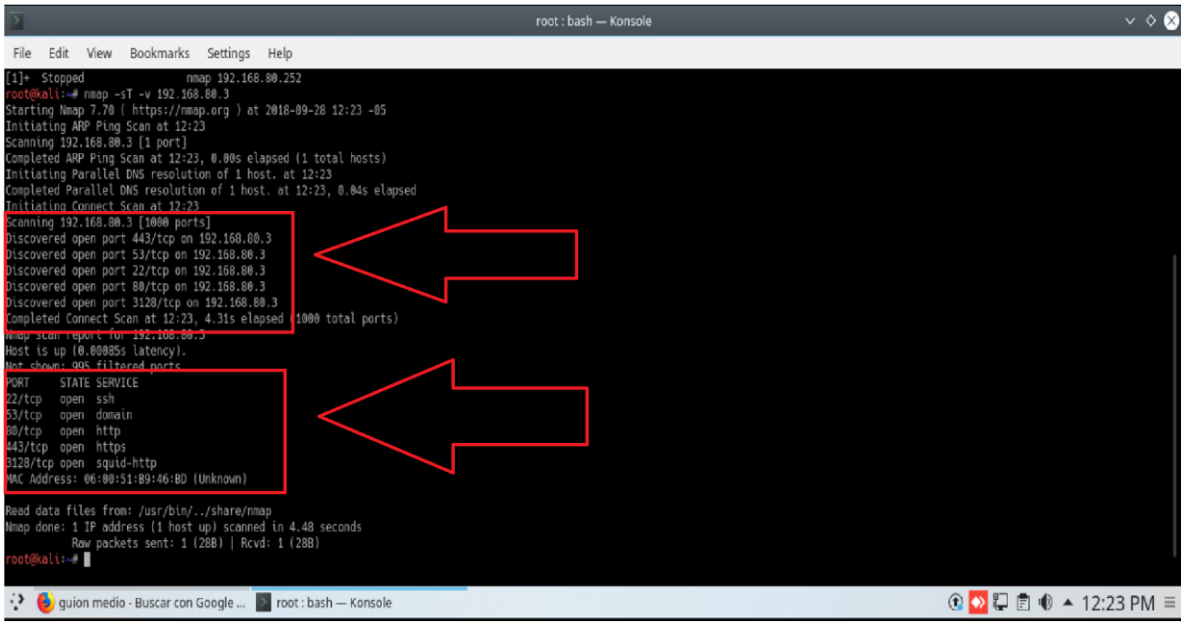


Ilustración 27. Escaneo de puertos Pfsense (Elaboración propia)

4.1.2 Fuerza Bruta

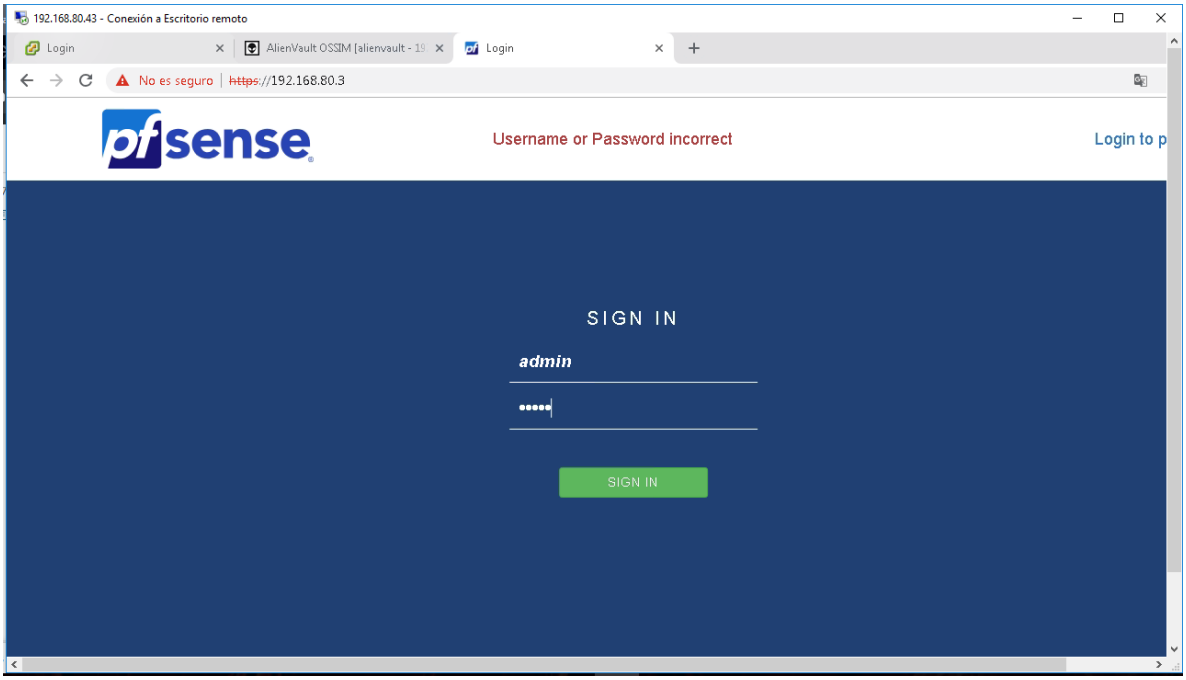


Ilustración 28. Ataque por fuerza bruta (Elaboración propia)

NOTA: para este ataque se hace una comprobación de tres contraseñas posibles escogidas aleatoriamente, con el fin de no saturar mucho el servidor.

4.1.3 Men In The Middle (MITM) mediante Ettercap

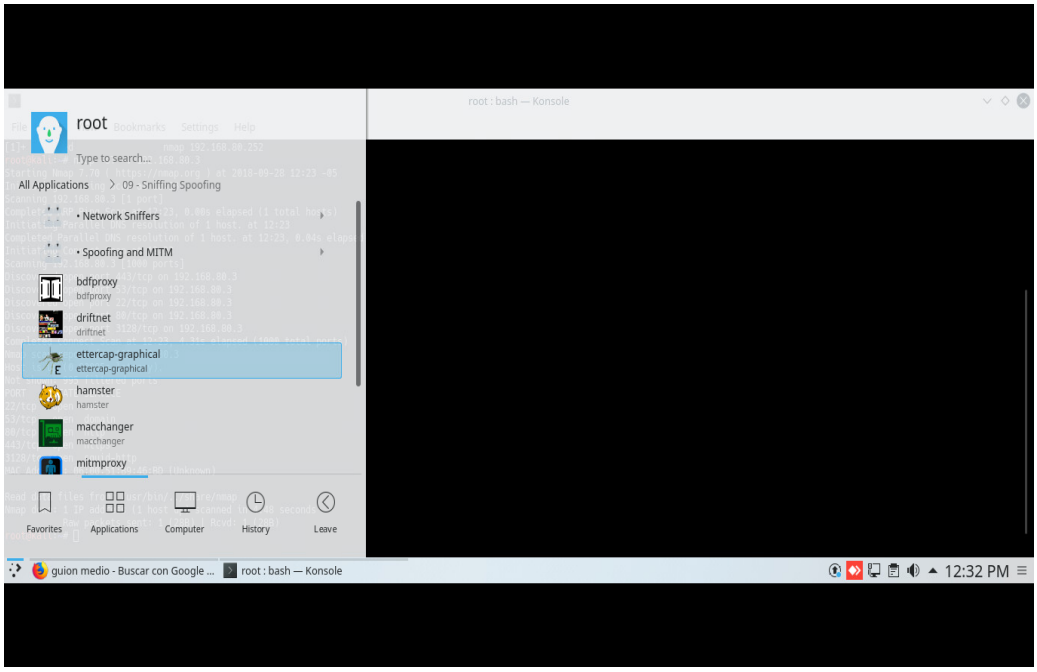


Ilustración 29. Selección de herramienta (Elaboración propia)

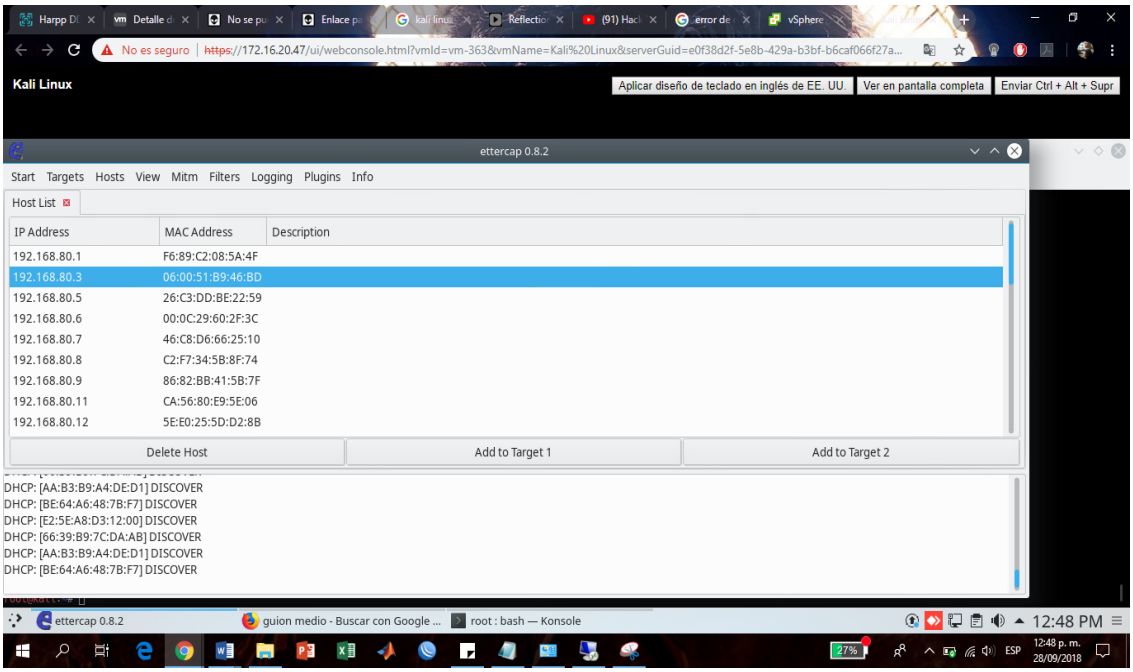


Ilustración 30. Selección de dispositivo a ser atacado mediante un escaneo previo (Elaboración propia)

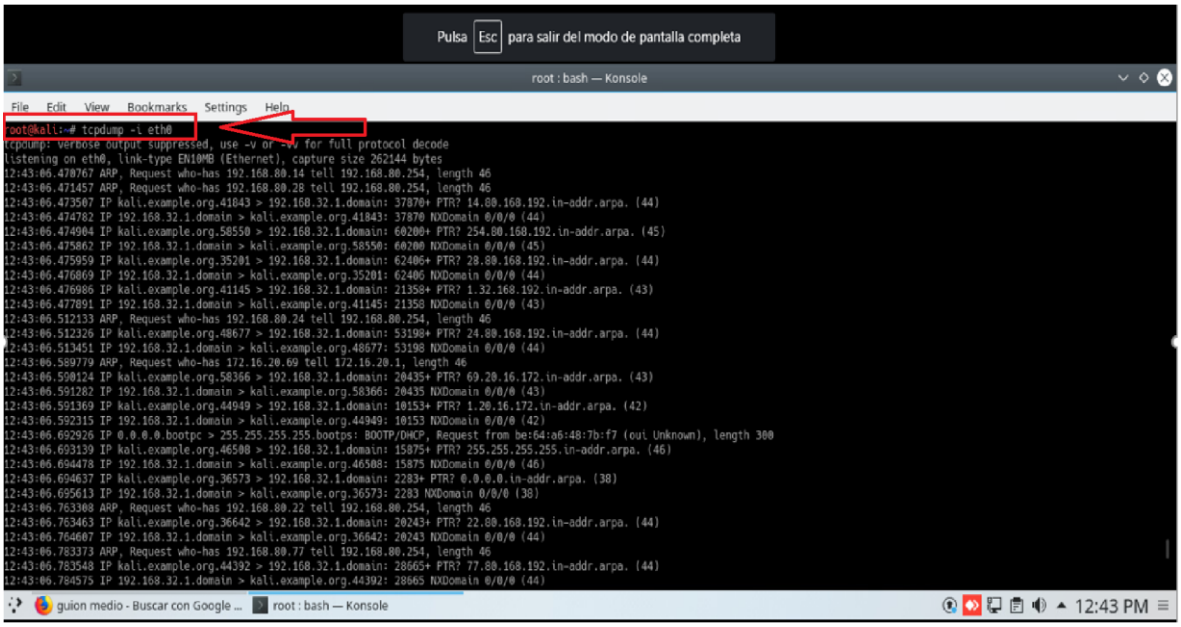


Ilustración 31. Ataque Men In The Middle (Elaboración propia)

4.1.4 Denegación de servicio mediante hping3

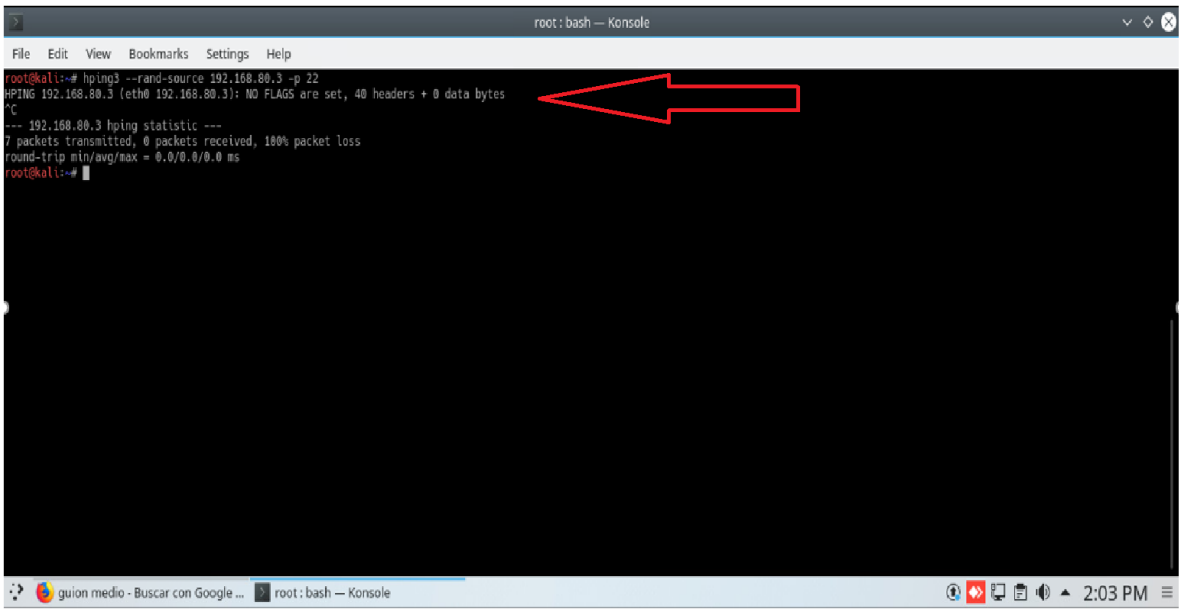


Ilustración 32. Ataque denegación de servicio por hping3 (Elaboración propia)

Nota: por efectos prácticos se decide no extenderse mucho con el tiempo de duración, ya que en una de las pruebas se dejó un lapso de tiempo largo y provoco la caída de la red.

4.1.5 Ataque Network Time Protocol (NTP)

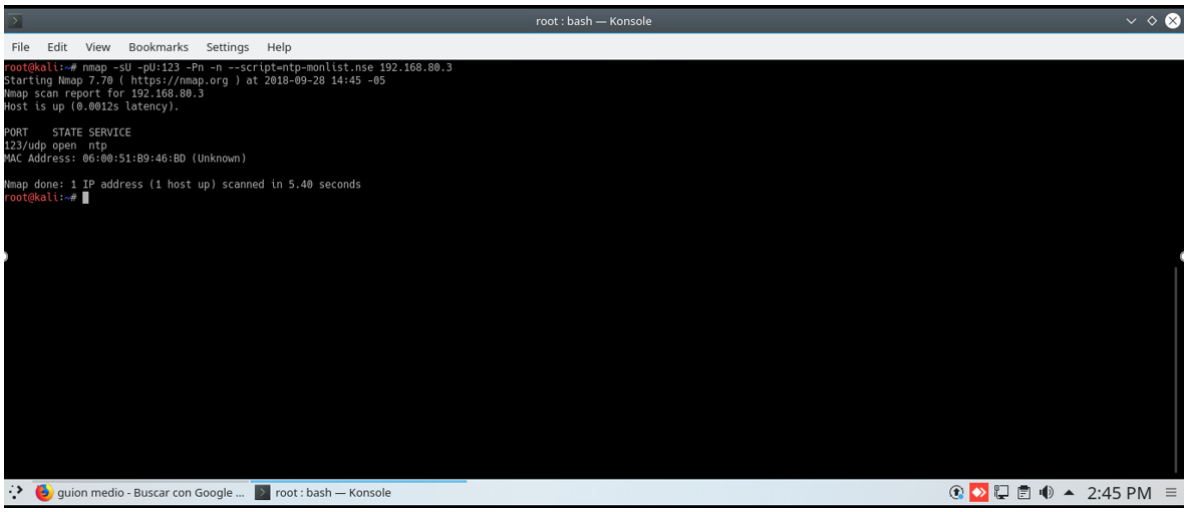


Ilustración 33. Ataque NTP mediante el uso de NMAP (Elaboración propia)

4.2 Comprobación de ataques

4.2.1 Comprobación escaneo de puertos

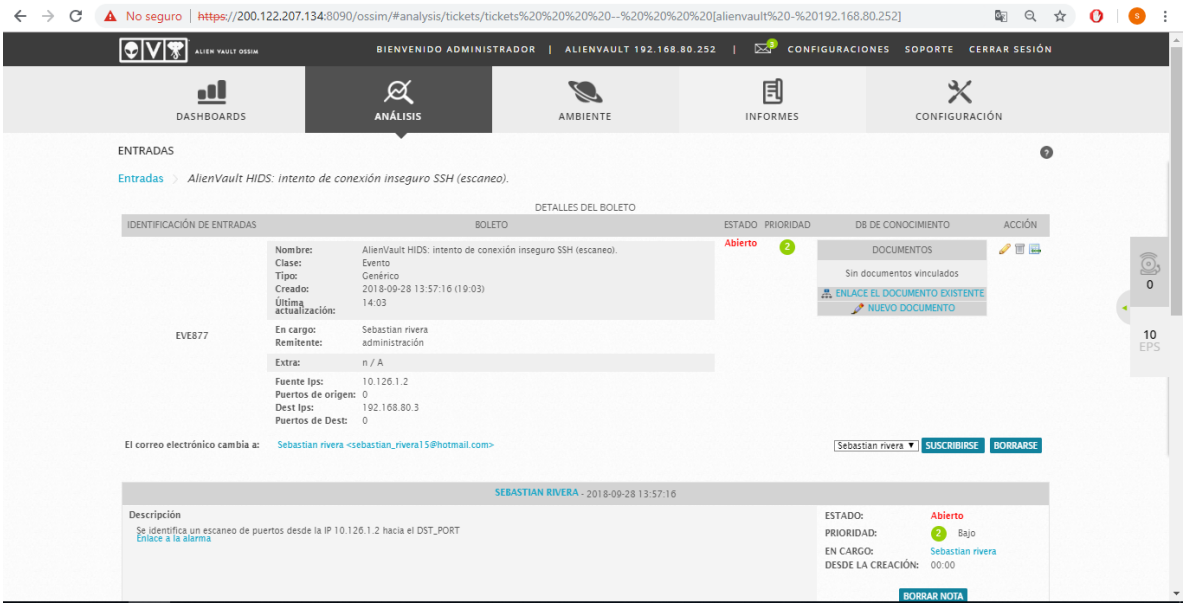


*Ilustración 34.*Alerta y descripción generada por el escaneo de puertos (Elaboración propia)

4.2.2 Comprobación ataque fuerza bruta

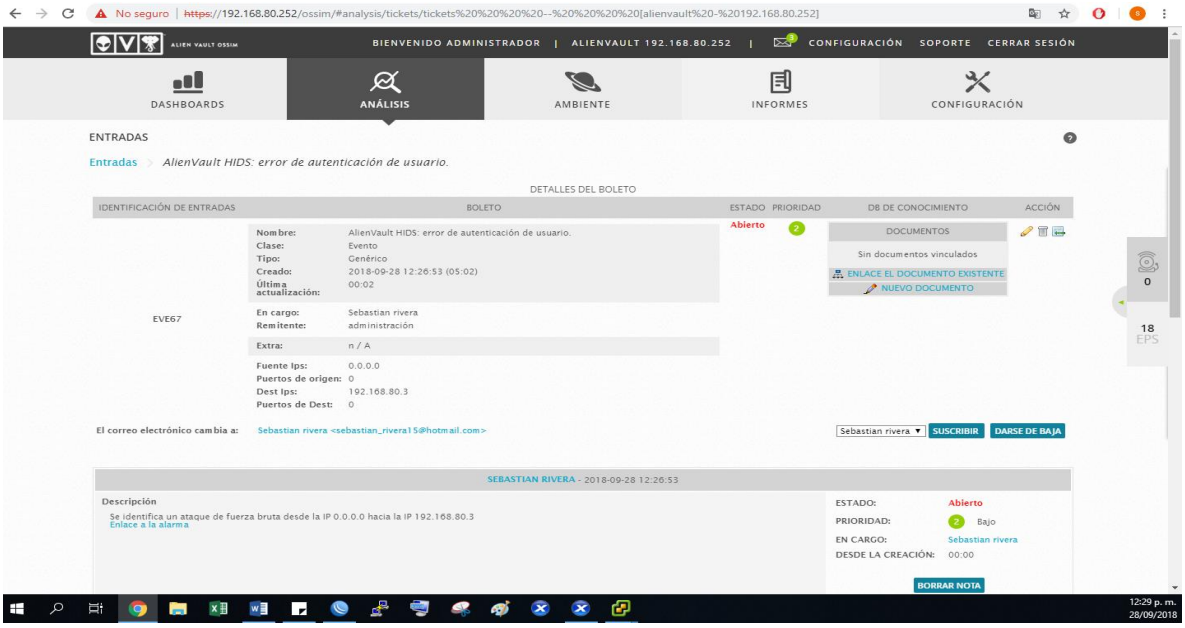


*Ilustración 35.*Alerta y descripción del ataque de fuerza bruta (Elaboración propia)

4.2.3 Comprobación ataque Men In The Middle (MITM)

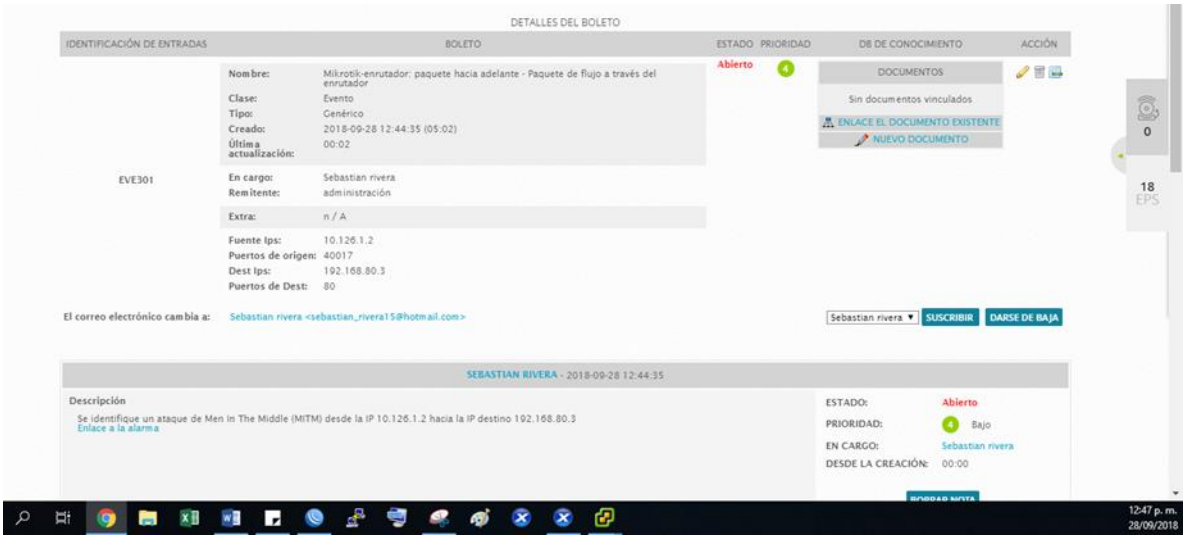


Ilustración 36. Alerta y descripción del ataque tipo Men In The Middle (Elaboración propia)

4.2.4 Comprobación ataque Denegación de servicio (DoS)

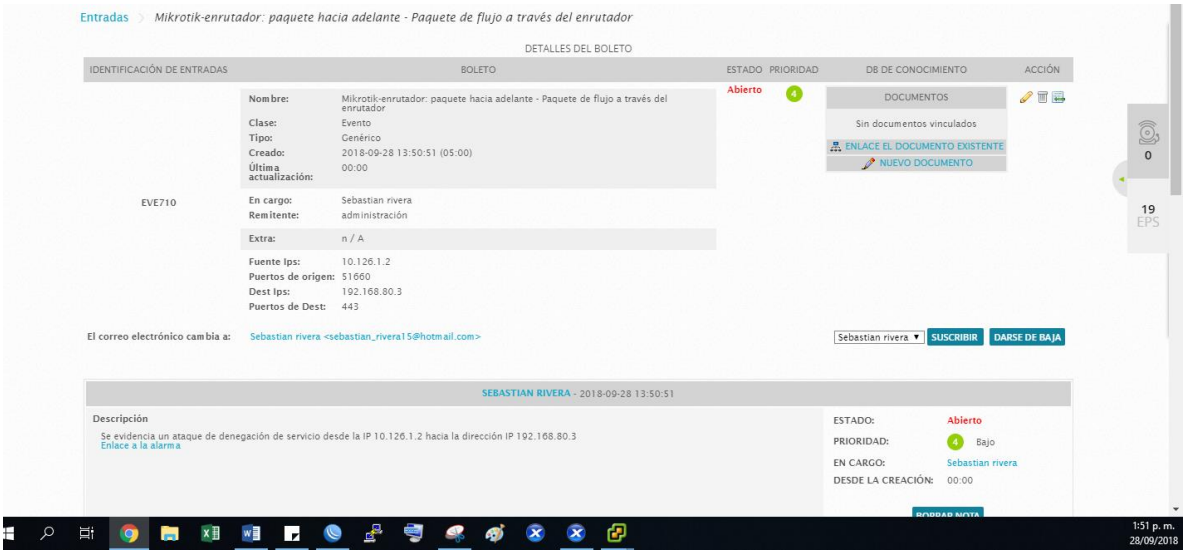


*Ilustración 37.*Alerta y descripción generada por el ataque de denegación de servicio (Elaboración propia)

4.2.5 Comprobación ataque NTP (Network Time Protocol)

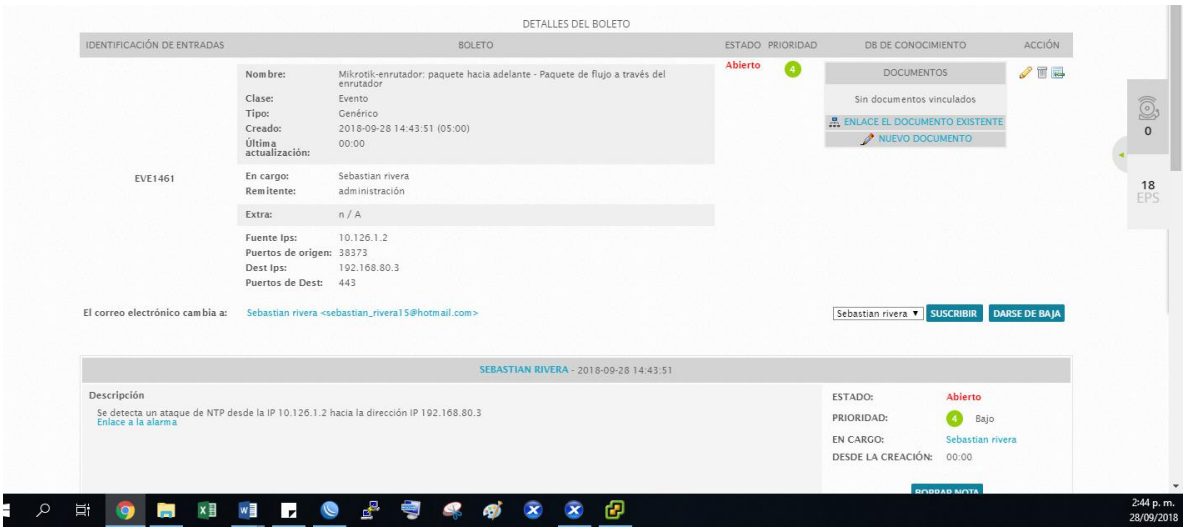


Ilustración 38. Alerta y descripción generada por el ataque de NTP (Elaboración propia)

Como se puede evidenciar las reglas de correlación han dado una respuesta efectiva, en vista que producen una alerta temprana acerca de los ataques que se le están haciendo al servidor. Esto también se puede analizar en la plataforma inicial que se muestra en la consola de administración, como se muestra en las siguientes secciones.

4.3 Análisis del monitoreo efectuado por el Alienvault

En un principio, el servidor al no tener ninguna configuración bien sea de reglas, acciones, dispositivos, entre otros, podíamos apreciar que las estadísticas de los tickets o alertas cubrían un 100% como se puede apreciar en la siguiente ilustración:

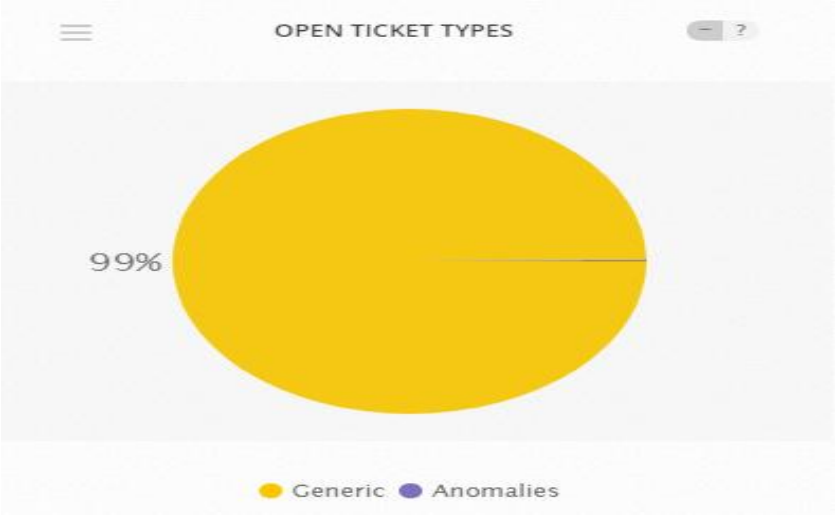


Ilustración 39. Eventos iniciales sin configuraciones Alienvault OSSIM (Diana Carolina Camacho, 2018)

Luego de realizar las configuraciones respectivas de las acciones, reglas de correlación, configuración de dispositivos para reenvío de logs y no siendo menos importante la implementación de los ataques informáticos, podíamos ver como cambiaban las estadísticas detallando cada porcentaje acerca de la concurrencia con se haya tenido.

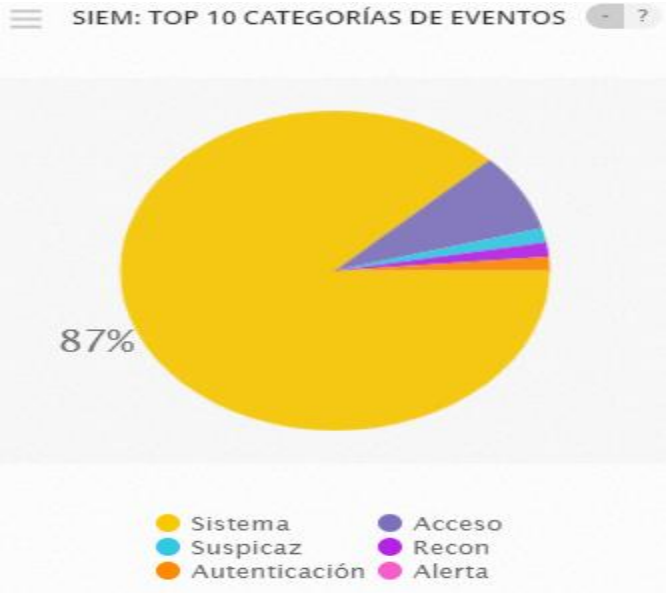


*Ilustración 40.*Estadisticas de monitoreo Alienvault OSSIM (Elaboración propia)

Apoyado en estas estadísticas podemos también evidenciar mediante la plataforma de administración cual fue el sensor que se evidencio más eventos de la siguiente manera:

Ilustración 41. Eventos registrados por sensor (Elaboración propia)

5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

5.1 CONCLUSIONES

Dado que en la actualidad las entidades que cuentan con dispositivos de red tienen un alto riesgo de padecer ataques informáticos, dichas entidades se ven en la tarea de mantener a salvo su información y los dispositivos de red; para ello es necesario contar con un sistema que detecte con anticipación los eventos que se presentan en dichos dispositivos y de esta forma lograr mitigar y porque no prevenir las posibles amenazas.

La conclusión fundamental es el logro de los objetivos del proyecto, en dónde se ejecutó el montaje, la configuración y afinación de las reglas de un correlacionador de eventos de seguridad basado en los riesgos de seguridad altos del bloque O, así mismo, se ejecutaron diferentes pruebas de seguridad y se evidenciaron en la consola del OSSIM, con base en esto, se deja un dispositivo configurado y probado para su posterior uso.

Es posible imaginar que una infraestructura está totalmente protegida con solo tener un antivirus en cada estación de trabajo, con un firewall que bloquee cada acceso no autorizado o cualquier dispositivo de seguridad que se encuentre dentro de la infraestructura. Estos dispositivos son eficientes y registran los acontecimientos que pasan por cada uno de los equipos, sin embargo, no es suficiente.

Un correlacionador de eventos es un complemento muy eficiente y tiene la capacidad de llevar un historial desde el día cero hasta el día de hoy con los dispositivos registrados; en él se pueden elaborar reglas y acciones con el fin de tener un entorno menos vulnerable.

Durante la implementación de OSSIM se presentaron algunos inconvenientes con el sensor ya que se encuentra deshabilitado y este estado no puede ser cambiado debido a que la versión Opensource de Alienvault que disponemos cuenta con un rol de analista, sin embargo, pese a que el sensor se encuentra deshabilitado el sigue recolectando los logs de los dispositivos; pero no muestra el reporte en la interfaz web por ejemplo el router de borde del bloque O, se configura el servicio Netflow en el servidor OSSIM y también realiza una configuración en el dispositivo, sin agente en el servidor con la dirección IP del router, sin embargo, esto no surtió efecto. Alienvault cuenta con una serie de plugins los cuales son habilitados por medio de la consola de comandos, una vez se activen los plugins necesarios, según el proveedor del dispositivo y el modelo los dispositivos podrán reportar los eventos en la interfaz web correctamente, para que de esta manera se les pueda ser aplicada una la configuración de las reglas de correlación.

La implementación de este recurso le da un valor más agregado a la red y la arquitectura del bloque O, ya que va contar con una herramienta la cual proveerá información valiosa de como es el comportamiento de la red en tiempo real. Además, de su capacidad y sencillez de poder analizar y reportar un diagnóstico acertado acerca de posibles eventualidades que puedan atentar contra la disponibilidad de la información.

5.2 RECOMENDACIONES

Es importante tener una base de conocimientos acertados acerca del funcionamiento y la infraestructura (físicos/lógicos) del sitio donde se pretende implementar el SIEM. En base a estos conocimientos es necesario hacer una escalabilidad o sondeo de riesgos para saber cuáles son los dispositivos que desempeñan un papel importante en la red y son los que proveen un servicio hacia los demás equipos.

5.3 TRABAJOS FUTUROS

A partir del trabajo realizado donde se logró implementar un SIEM con varias reglas de correlación se sugiere un trabajo a futuro donde se incluyan nuevas tecnologías como por ejemplo cloud computing o a nivel de aplicaciones, aquí se debe realizar un análisis más detallado sobre las vulnerabilidades que se presentan en estas nuevas tecnologías que puedan ser implementadas en el laboratorio de convergentes del ITM; allí se harán una serie de reglas de correlación que cumplan con las necesidades pactadas.

Un futuro trabajo podría ser la implementación de una infraestructura de cloud computing debido a que un SIEM como correlacionador de eventos es una pieza fundamental al momento de unificarlo con el firewall perimetral que se está implementando en la actualidad para conseguir un entorno seguro de cloud computing. Un SIEM es un gran aliado ya que con la metodología presentada en el actual trabajo se puede explotar al máximo su funcionalidad junto con cloud computing, debido a que el SIEM actuaría como una capa que está cubriendo a varios de los dispositivos o sistemas que se encuentran en la nube para protegerlos.

REFERENCIAS

Alienvault. (s.f.). *www.alientvault.com*. Obtenido de www.alientvault.com: https://www.alienvault.com/documentation/usm-anywhere/user-guide/user-management/rbac.htm

Arango, J. D. (2016). *IMPLEMENTACION DE UN GESTOR DE SEGURIDAD DE LA INFORMACION Y GESTOR DE EVENTOS (SIEM).* Medellín: Universidad San Buenaventura.

Benedict, J. (2016). *xenserver.org*. Obtenido de xenserver.org: https://xenserver.org/blog/entry/log-rotation-and-syslog-forwarding.html

Boada, P. W. (2016). *Análisis y Selección de una herramienta para administración y obtención de información de eventos criticos de seguridad informatica para la infraestructura del Ministerio de Telecomunicaciones y de la sociedad de la informacion- MINTEL.* Quito: PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR.

Diana Carolina Camacho, L. J. (2018). *Implementación de una arquitectura de correlación de eventos para la mitigación de riesgos informaticos de una infraestructura de servidres virtuales del laboratorio de redes convergentes del ITM.* Medellin.

Franco, D. A., Perea, J., & Puello, P. (2012). Metodología para la detección de vulnerabilidades en redes de datos. *Información Tecnologica*.

Manuel Rodriguez Lopez, C. P. (2013). *una galicia moderna.* Obtenido de una galicia moderna: http://www.unagaliciamoderna.com/Eawp/coldata/upload/mapa_de_riesgos_19_06_13.pdf

Mendoza, A. (27 de noviembre de 2017). *www.gb-advisors.com*. Obtenido de www.gb-advisors.com: http://www.gb-advisors.com/es/cuadrante-de-gartner/

Mesa, S. L. (25 de febrero de 2017). *OSSIM Ethical Hacking © 2017*. Obtenido de OSSIM Ethical Hacking © 2017: https://www.youtube.com/watch?v=5NtQSL3SKlY&t=269s

Munera, D. C.-A. (2007). *Guia metodologica para la gestión centralizada de registro de eventos de seguridad en Pymes.* Bogota.

Network Management Software. (2018). Obtenido de Network Management Software: https://www.networkmanagementsoftware.com/what-is-syslog/

Pardo, D. (17 de septiembre de 2018). *blog.pandorafms.org*. Obtenido de blog.pandorafms.org: https://blog.pandorafms.org/es/que-es-snmp/

S. Sandeep Sekharan, C. A. (2017). Creación de perfiles de herramientas SIEM y motores de correlación para análisis de seguridad. *Creación de perfiles de herramientas SIEM y motores de correlación para análisis de seguridad* (pág. 5). Chennai: IEEE.

APÉNDICE

Apéndice A: Instalación básica de Alienvault OSSIM

1. Se selecciona la primera opción.

Ilustración 42. Instalación inicial OSSIM (Mesa, 2017) (Diana Carolina Camacho, 2018)

2. En este segundo paso seleccionamos el lenguaje que más senos acomode para entender, ubicación y demás parámetros regionales.

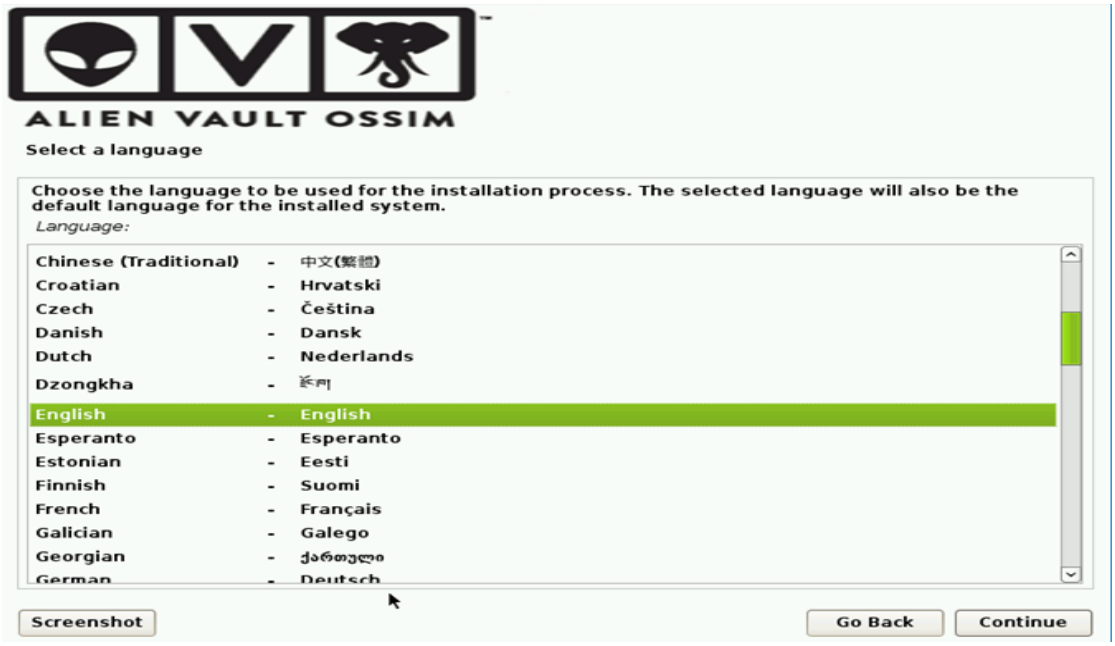


Ilustración 43. Selección del lenguaje OSSIM (Mesa, 2017) (Diana Carolina Camacho, 2018)

Ilustración 44. Selección de la ubicación OSSIM (Mesa, 2017) (Diana Carolina Camacho, 2018)

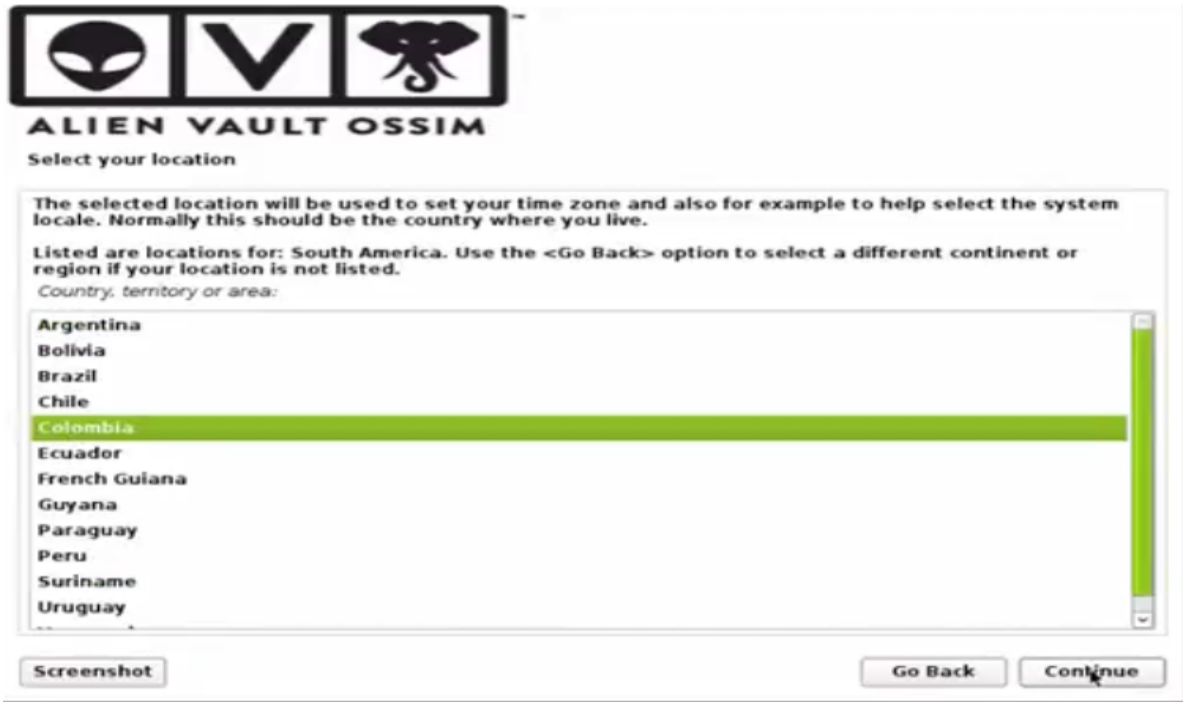


Ilustración 45. Selección de la ubicación OSSIM *(Mesa, 2017)*

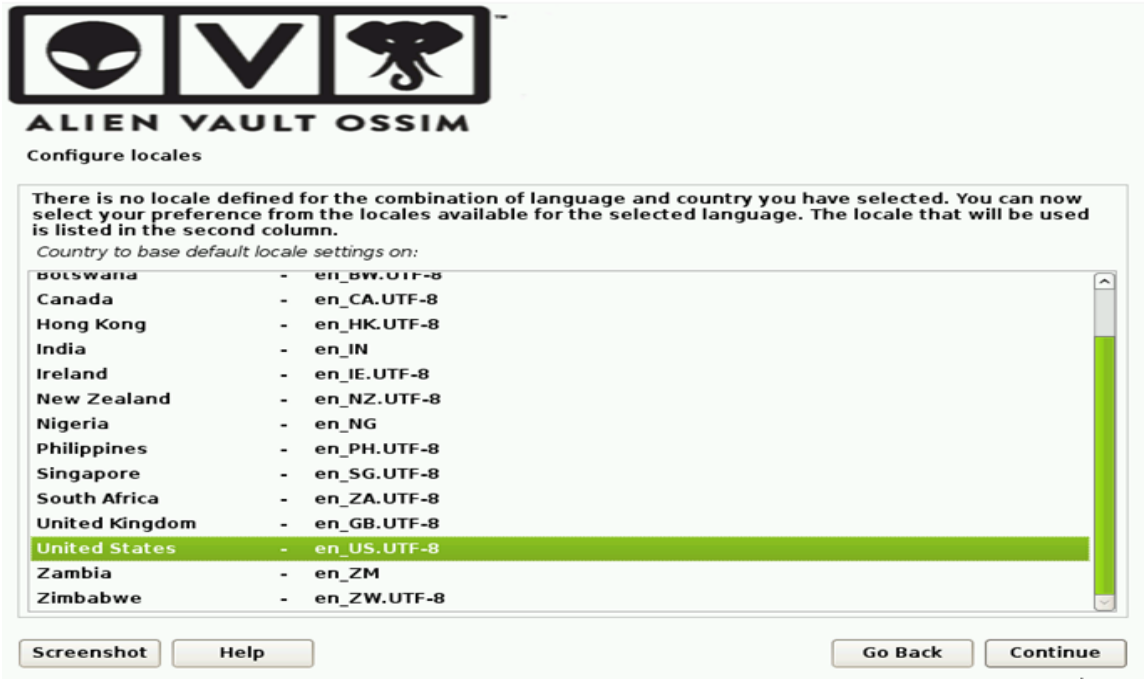


Ilustración 46. Configuración parámetros regionales OSSIM *(Mesa, 2017) (Diana Carolina Camacho, 2018)*

3. En este paso se selecciona el tipo de teclado con el que se va trabajar.

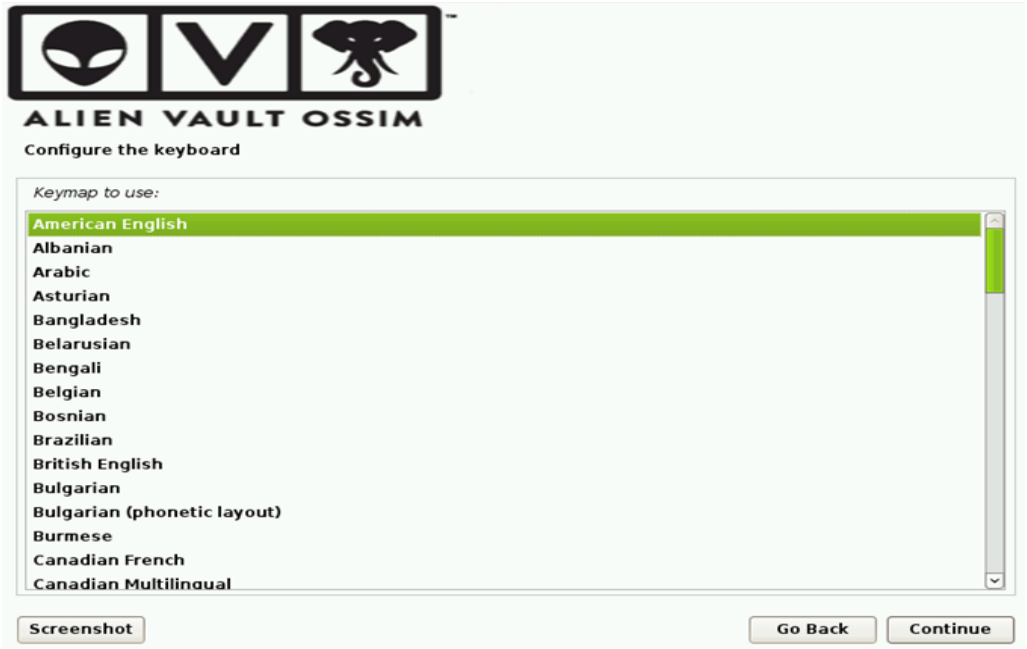


Ilustración 47. Configuración teclado OSSIM *(Mesa, 2017) (Diana Carolina Camacho, 2018)*

4. Para esta sección se debe configurar la dirección IP, mascara y Gateway del servidor. Es importante tener conocimiento de estos parámetros, para evitar conflictos y malas configuraciones de red.

Ilustración 48. Configuración interfaz de red OSSIM *(Mesa, 2017)*

Ilustración 49.Asignación de dirección IP OSSIM *(Mesa, 2017)*

Ilustración 50.Mascara de red OSSIM *(Mesa, 2017) (Diana Carolina Camacho, 2018)*

Ilustración 51. Gateway OSSIM (Mesa, 2017) *(Diana Carolina Camacho, 2018)*

5. Seguidamente se configuran la contraseña del usuario root, el cual servirá de gran ayuda para configuraciones por consola, a través de SSH.

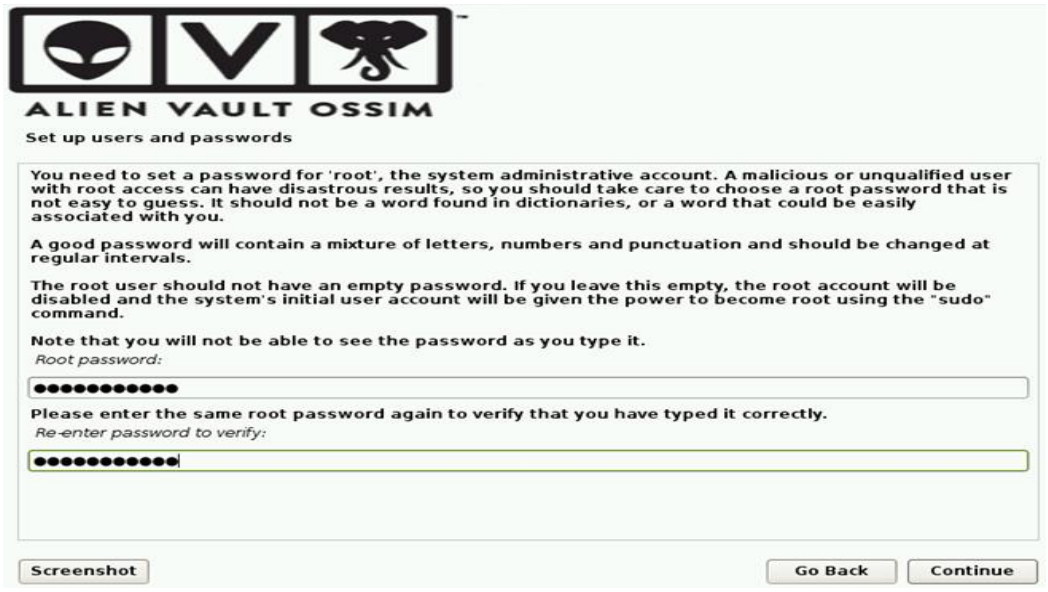


Ilustración 52. Configuración de contraseña usuario root *(Mesa, 2017) (Diana Carolina Camacho, 2018)*

Finalmente, comenzará la instalación. Es importante tener paciencia ya que OSSIM es un poco demorado en su instalación por la cantidad de recursos que requiere.

Ilustración 53. Finalización de la instalación OSSIM *(Mesa, 2017) (Diana Carolina Camacho, 2018)*

Apéndice B: Configuración de reenvío de logs hacia el servidor OSSIM en cada dispositivo que alertado en el mapa de riesgos.

1. Router Mikrotik

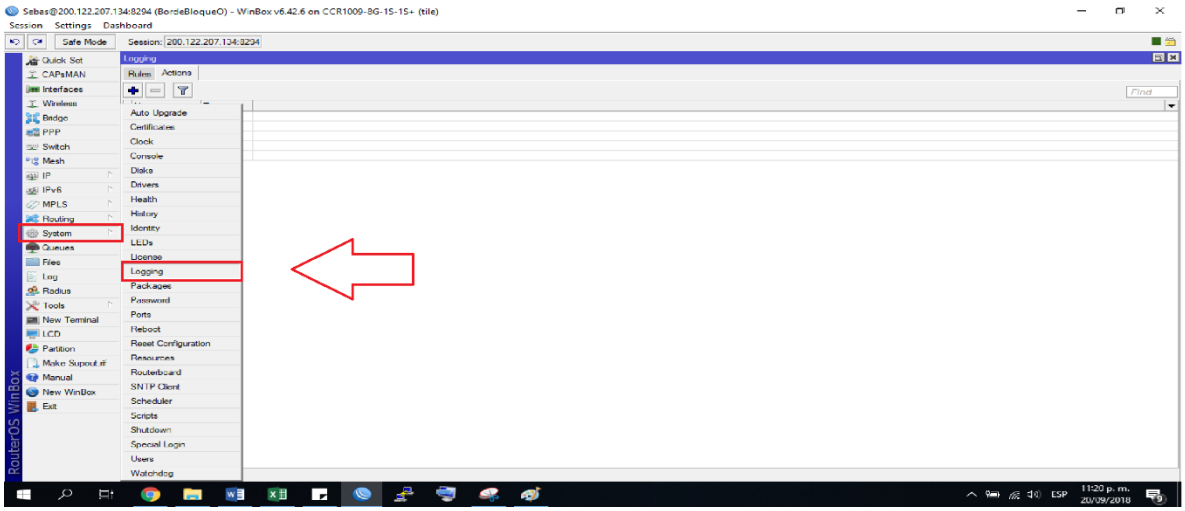


Ilustración 54. Configuración reenvío syslog router Mikrotik (Elaboración propia)

Luego procedemos a configurar una acción con la dirección por donde se hará la recolección de logs, de la siguiente manera.

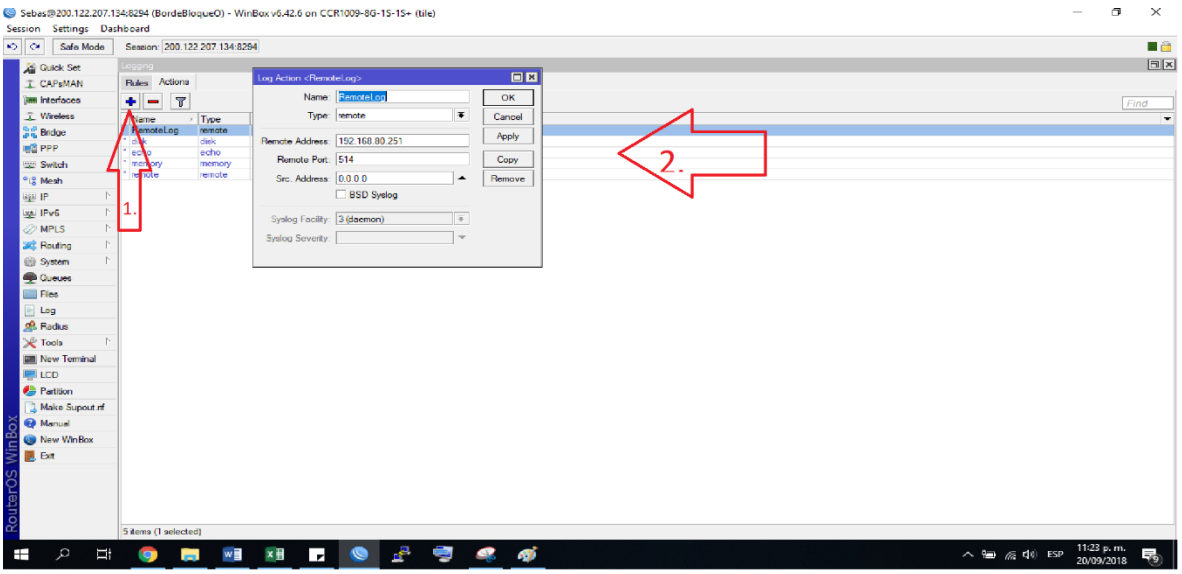


Ilustración 55. Acción para reenvío de logs router Mikrotik (Elaboración propia)

Luego esa acción ya creada la podemos asignar a cualquiera de las reglas que estén por defecto en el router, de la siguiente manera

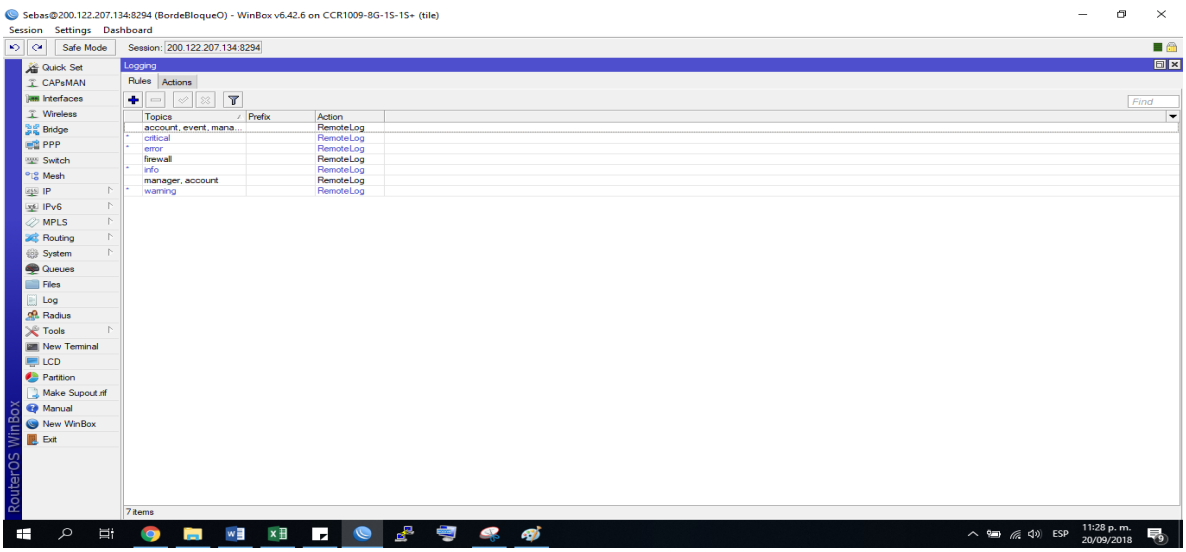


Ilustración 56. Aplicación de la acción creada router Mikrotik (Elaboración propia)

2. Hipervisor vSphere

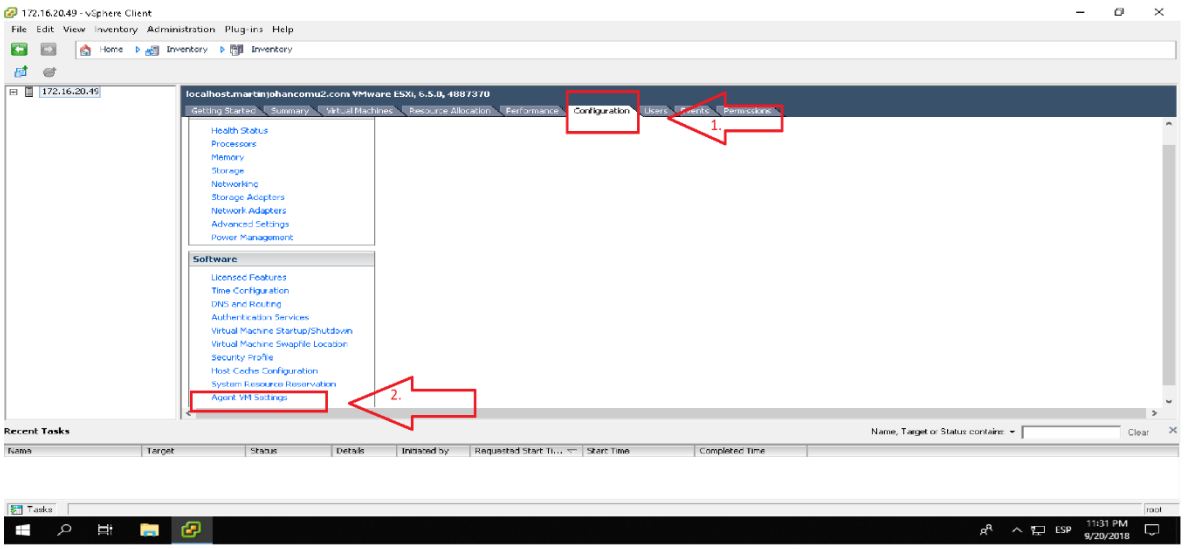


Ilustración 57. Configuración inicial Hipervisor vSphere (Elaboración propia)

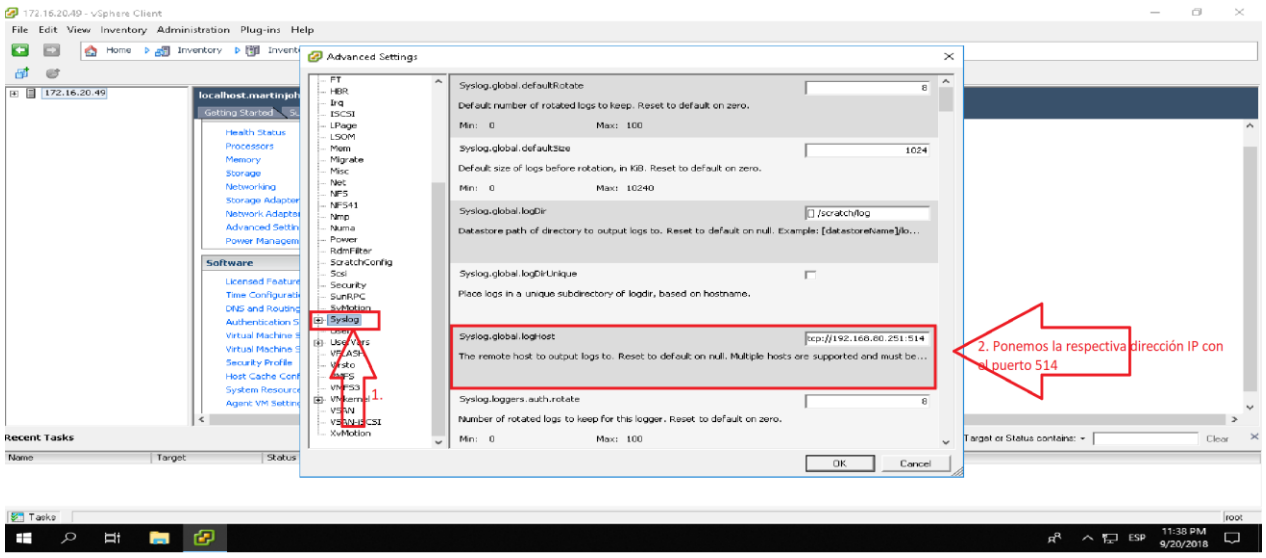


Ilustración 58. Asignación de dirección IP para recolección de Logs (Elaboración propia)

NOTA: El puerto 514 es el que utiliza OSSIM para la recolección de log.

3. Hipervisor Xenserver

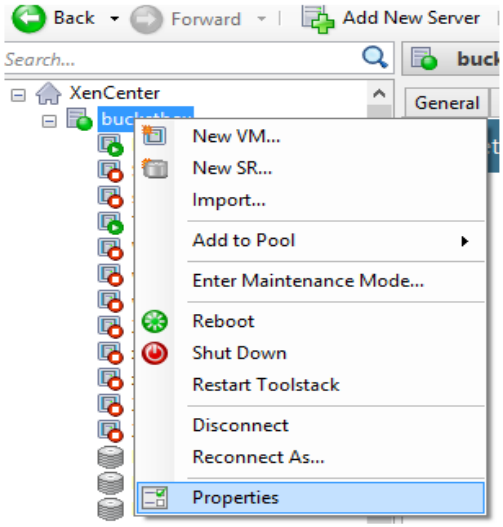


Ilustración 59. Propiedades Hipervisor Xenserver para redirección de logs *(Benedict, 2016)*

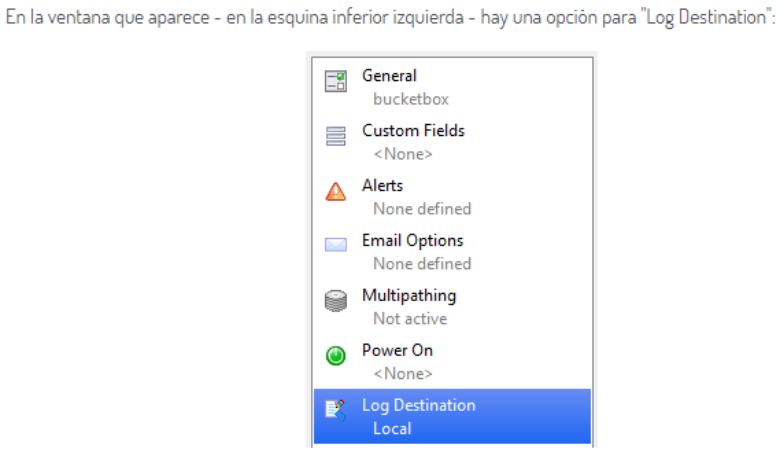


Ilustración 60. Redirección de logs Xenserver (Benedict, 2016)

Ilustración 61. Configuración IP para recolección de log Xenserver (Benedict, 2016)

4. Hipervisor Proxmox

Para este dispositivo en especial no se hará de manera gráfica, sino con el fin de motivar el aprendizaje se hará por medio de la consola configurando Rsyslog de la siguiente manera:

Rsyslog es un mecanismo usado para el registro syslog. Tiene la capacidad de entregar una cantidad considerable de mensajes por segundo a diferentes destinos sean remotos o locales cuando se aplica un proceso limitado. (Diana Carolina Camacho, 2018)

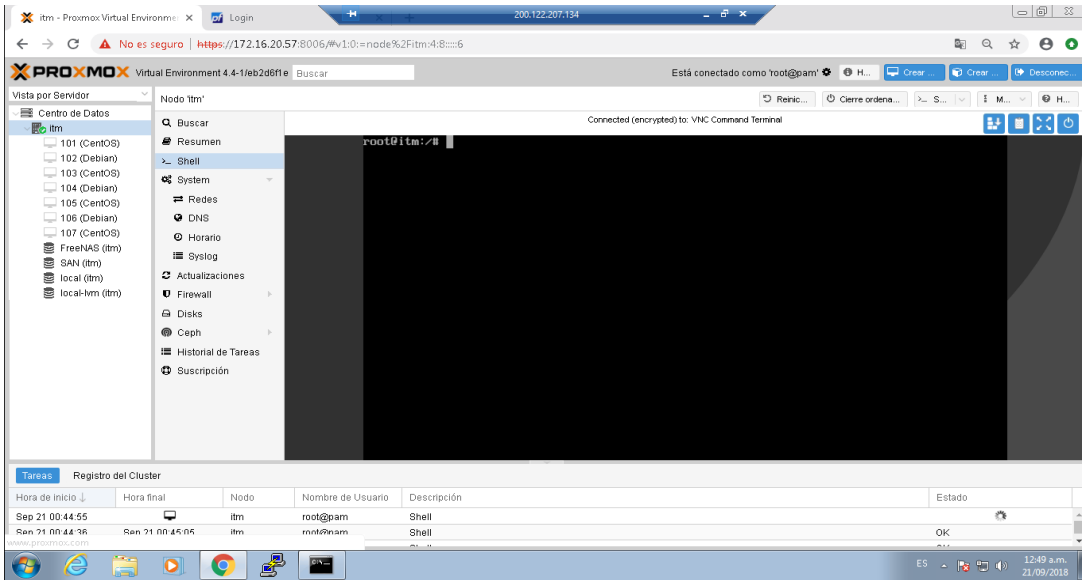


Ilustración 62. Consola Hipervisor Proxmox (Elaboración propia)

Descargamos Rsyslog con: *apt-get install rsyslog*

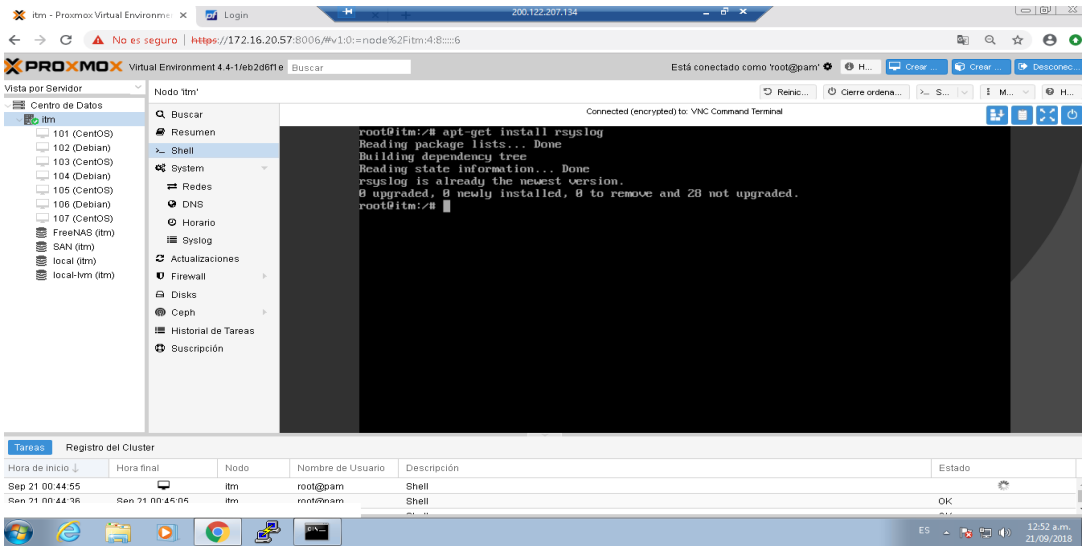


Ilustración 63. Instalación de Rsyslog en Hipervisor Proxmox (Elaboración propia)

Miramos en qué estado está el servicio rsyslog con: *status rsyslog.service*

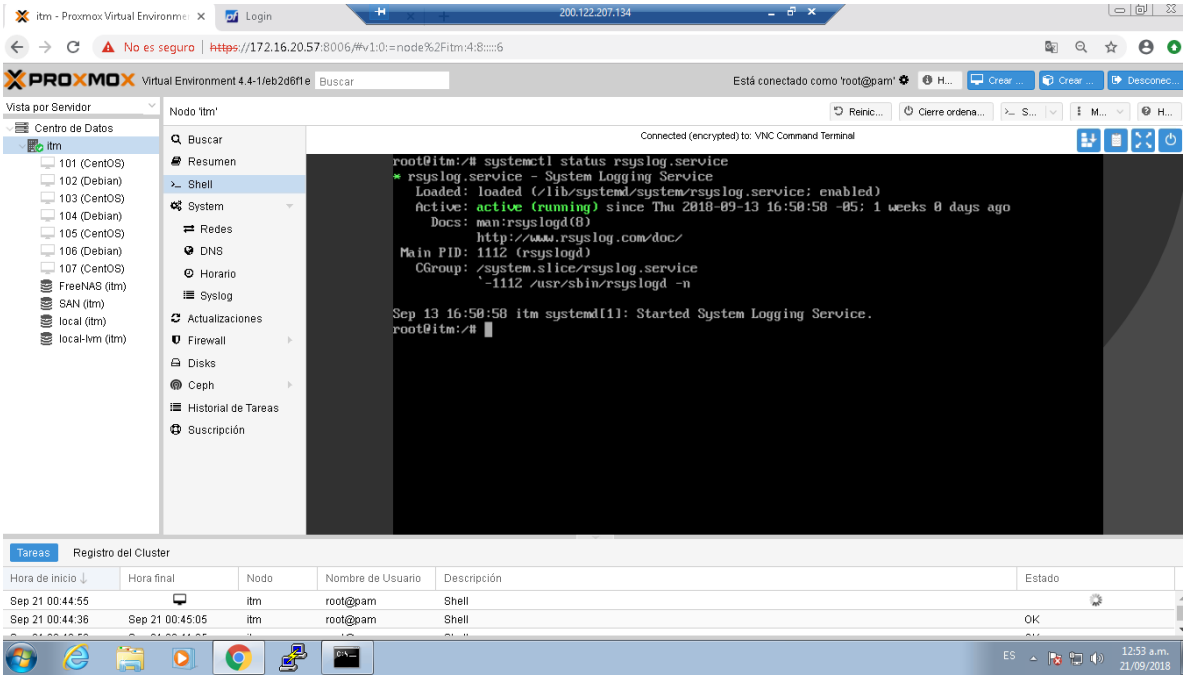


Ilustración 64. Estatus Rsyslog Hipervisor Proxmox (Elaboración propia)

Ahora procedemos a hacer la configuración de la IP a la que serán redireccionados los mensajes syslog. Primero entramos en la ruta: *cd /etc/rsyslog. d*

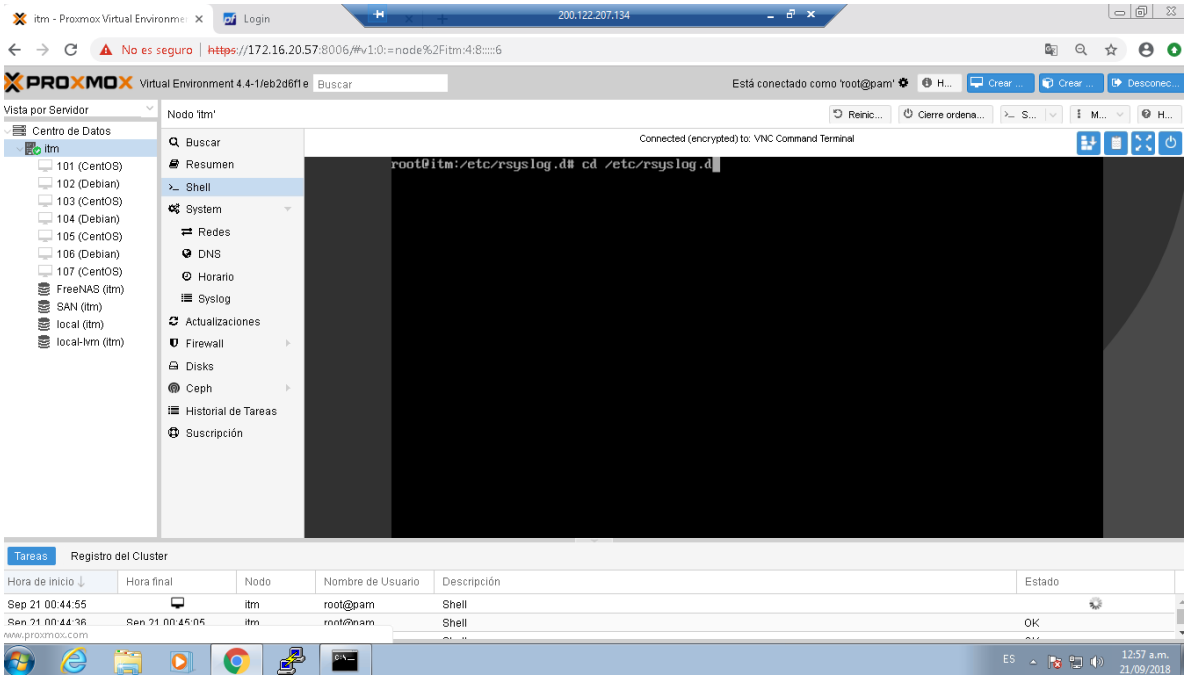


Ilustración 65. Ruta de configuración IP remota (Elaboración propia)

Después de estar parados en esa ruta ponemos este archivo *nano alienvault.conf* que es donde se agregará la IP correspondiente.

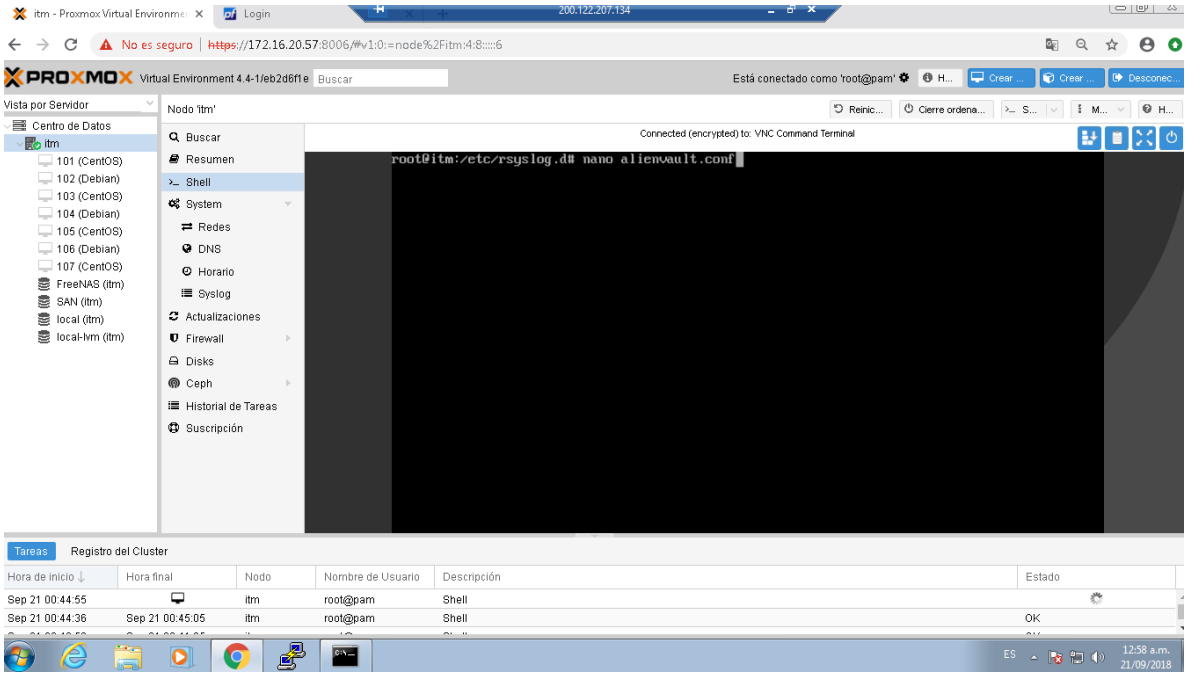


Ilustración 66. nano alienvault.conf (Elaboración propia)

En el archivo que editaremos pondremos exactamente la dirección IP remota: ***. * @192.168.80.251**

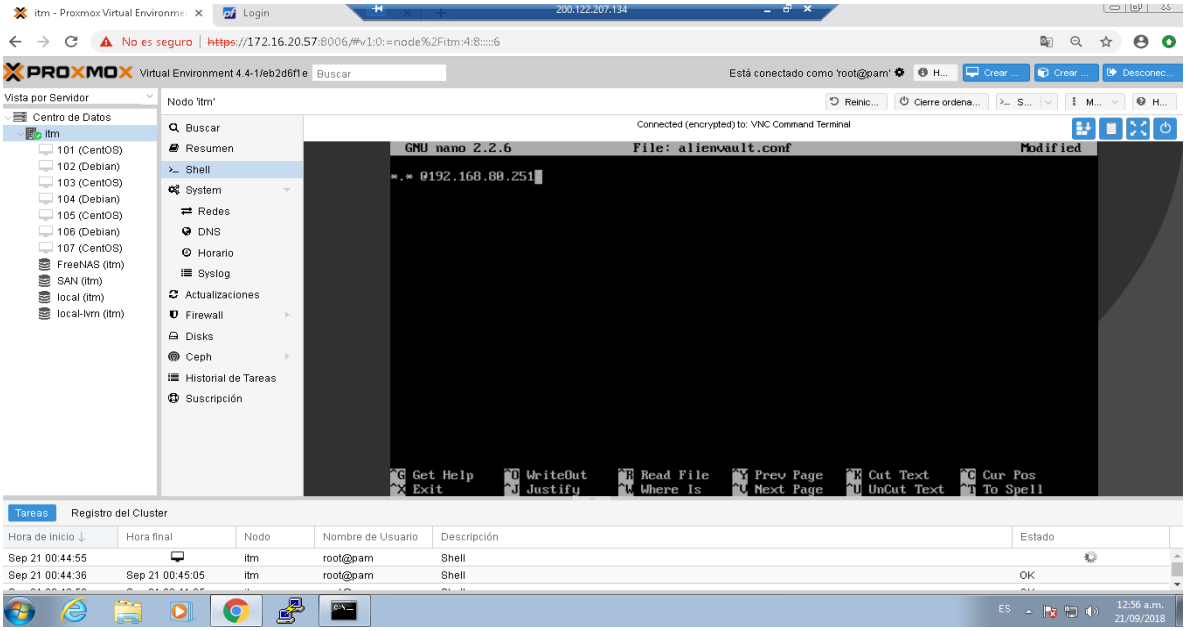


Ilustración 67. Configuración IP remota (Elaboración propia)

Finalmente, solo reiniciamos el servicio con *service rsyslog restart*

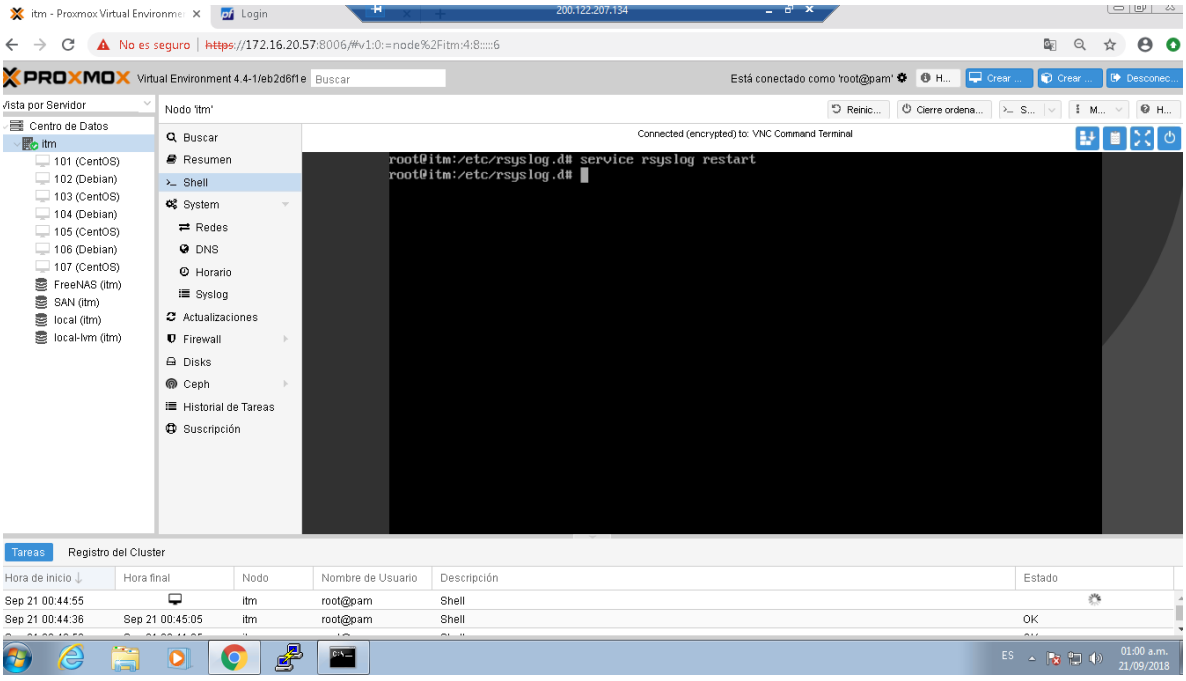


Ilustración 68. Reinicio de rsyslog (Elaboración propia)

5. Pfsense

Inicialmente entrados al dashboard del dispositivo y nos vamos para la opción status, como se muestra en la siguiente ilustración

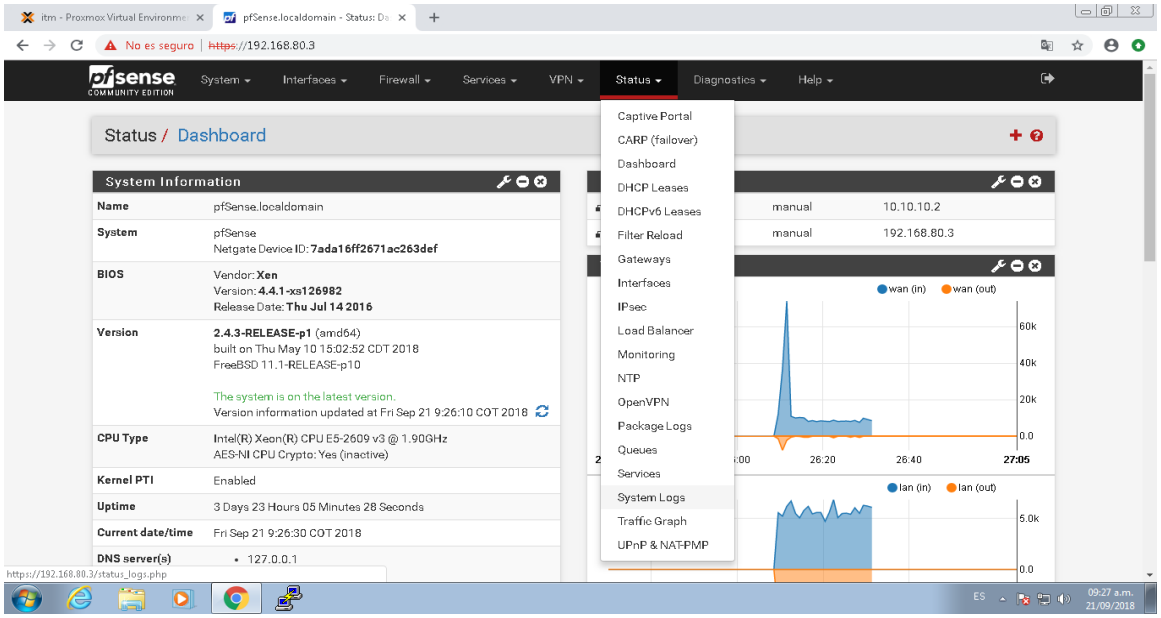


Ilustración 69. Dashboard Pfsense (Elaboración propia)

Luego nos vamos para la opción *settings.* En la parte de abajo aparecerá la opción*: remote logs,* allí es donde agregaremos la dirección IP para recolección de logs

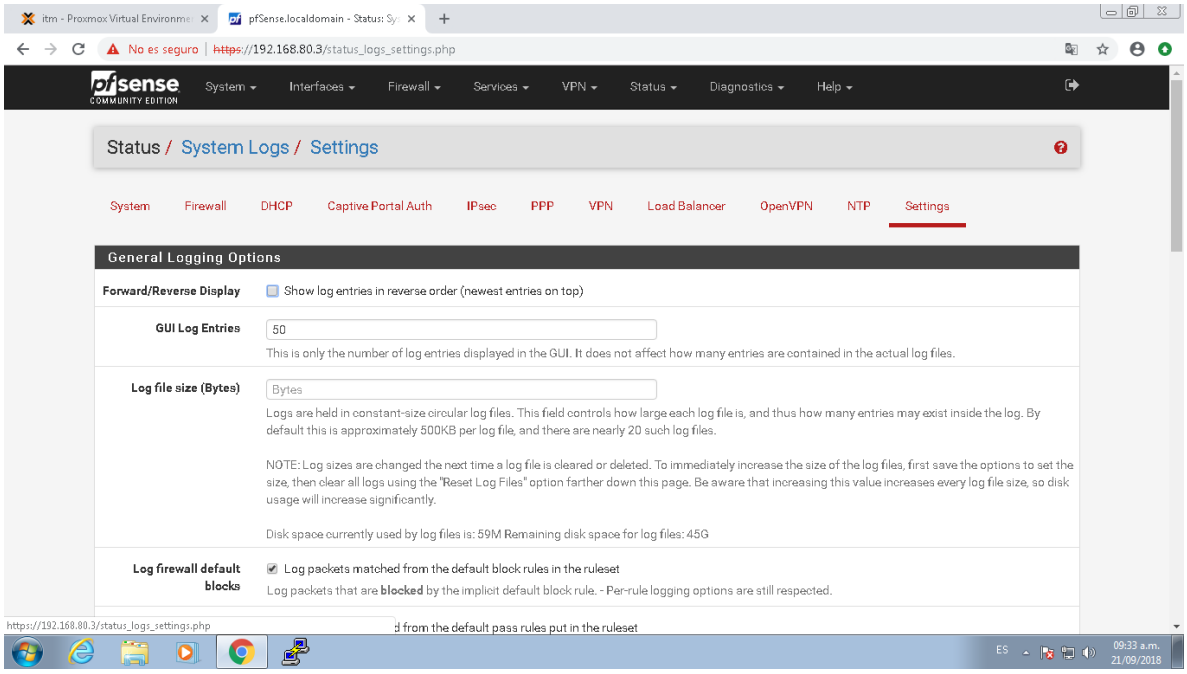


Ilustración 70. Opciones de configuración remote logs Pfsense (Elaboración propia)

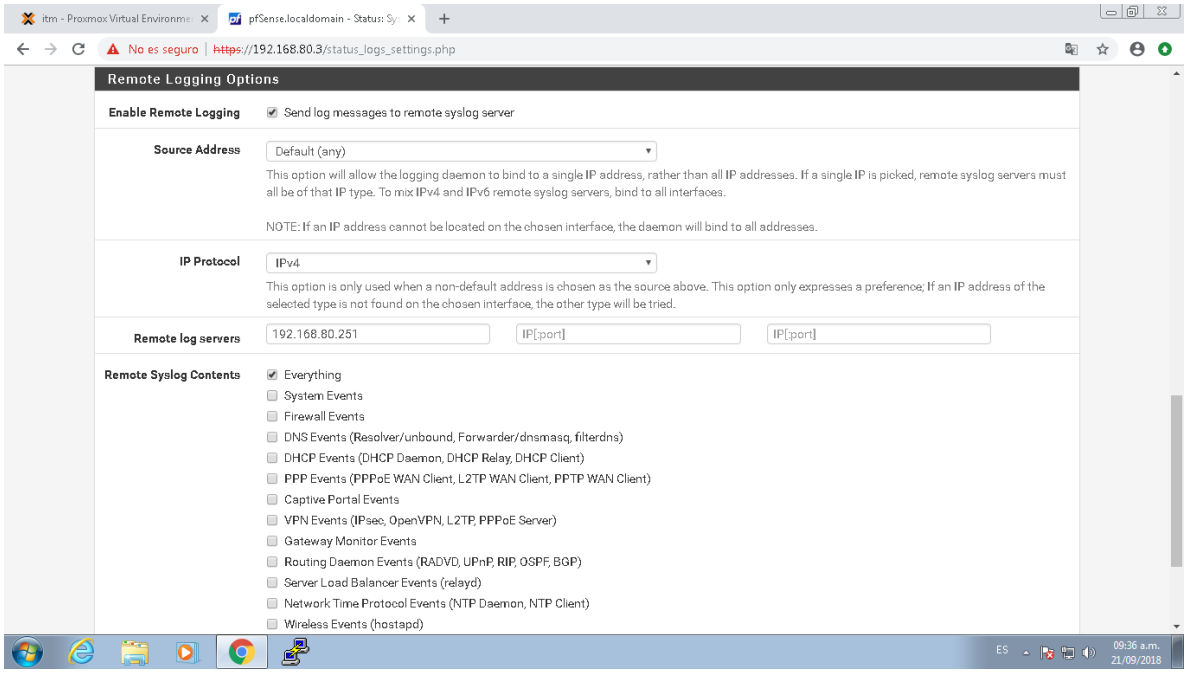


Ilustración 71. Configuración remote log Pfsense (Elaboración propia)

Apéndice C: Configuración reglas de correlación

Es importante tener en cuenta que para cada regla de correlación que se es configurada, debe estar sujeta a una acción que describa la clase de alerta que está sucediendo en el momento que se abre el ticket. Estas acciones en el momento de la configuración de la regla de correlación se configuran como una consecuencia. Seguidamente se procede a la configuración de cada una de las acciones que van sujetas a cada regla de correlación

- **Acciones**

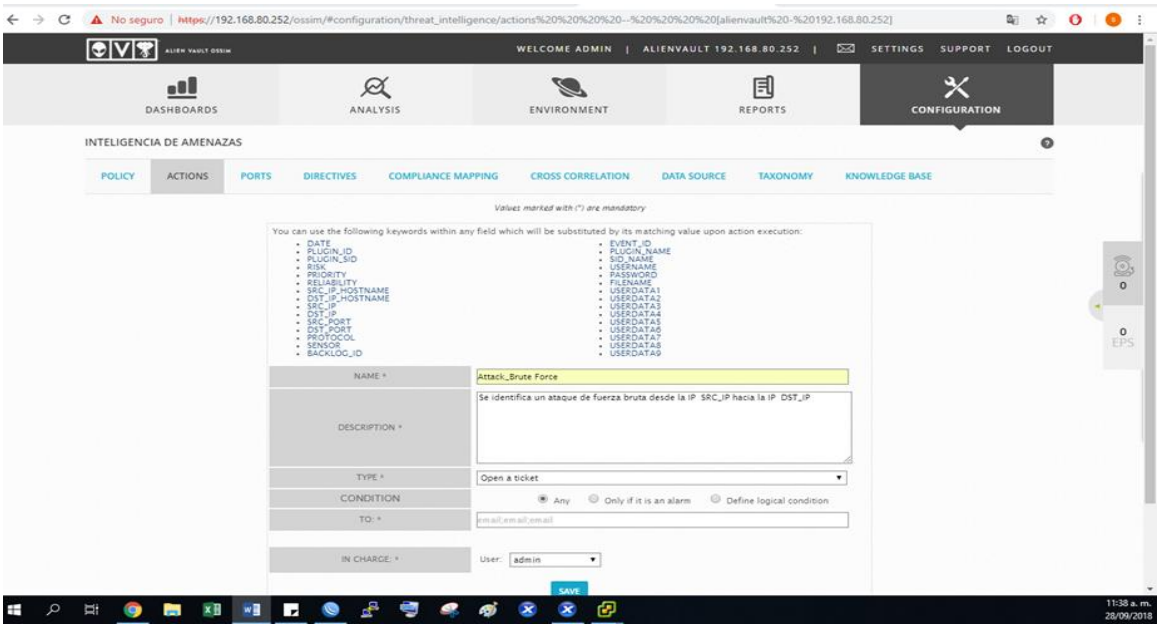


Ilustración 72. Acción para ataque fuerza bruta (Elaboración propia)

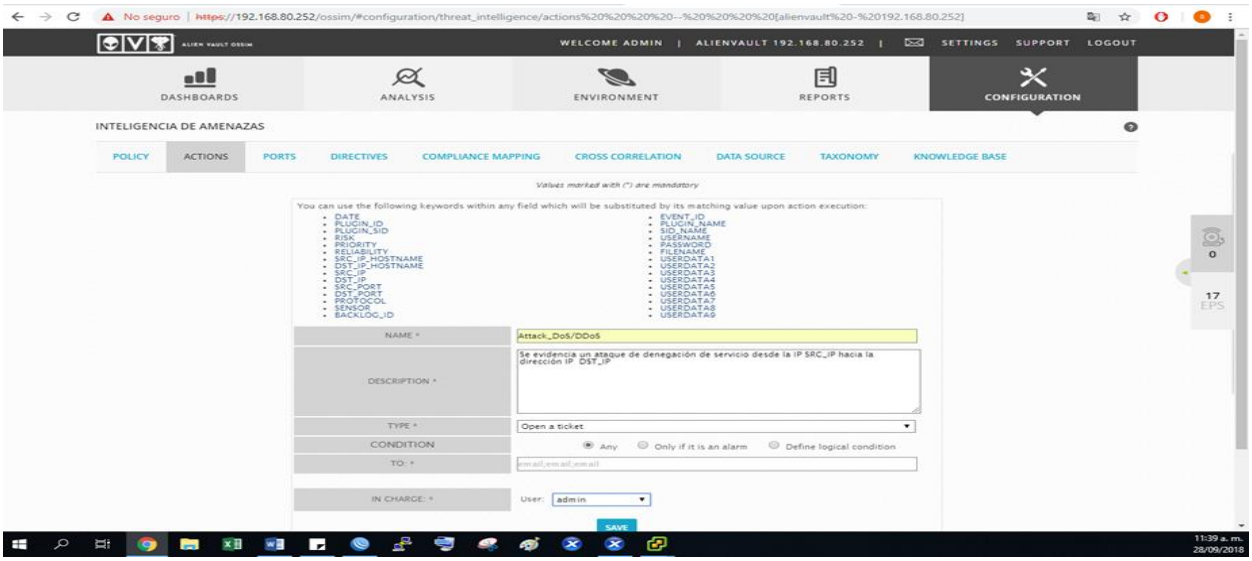


Ilustración 73. Acción para ataque DoS (Elaboración propia)

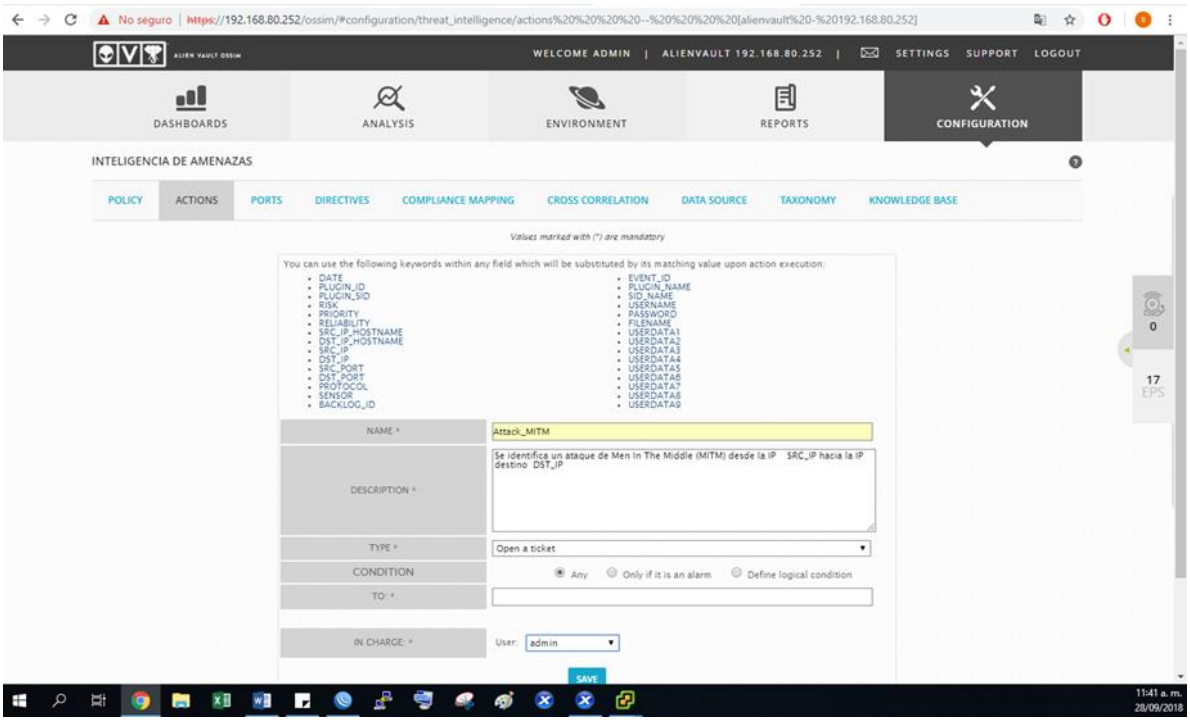


Ilustración 74. Acción para ataque Men In The Middle (Elaboración propia)

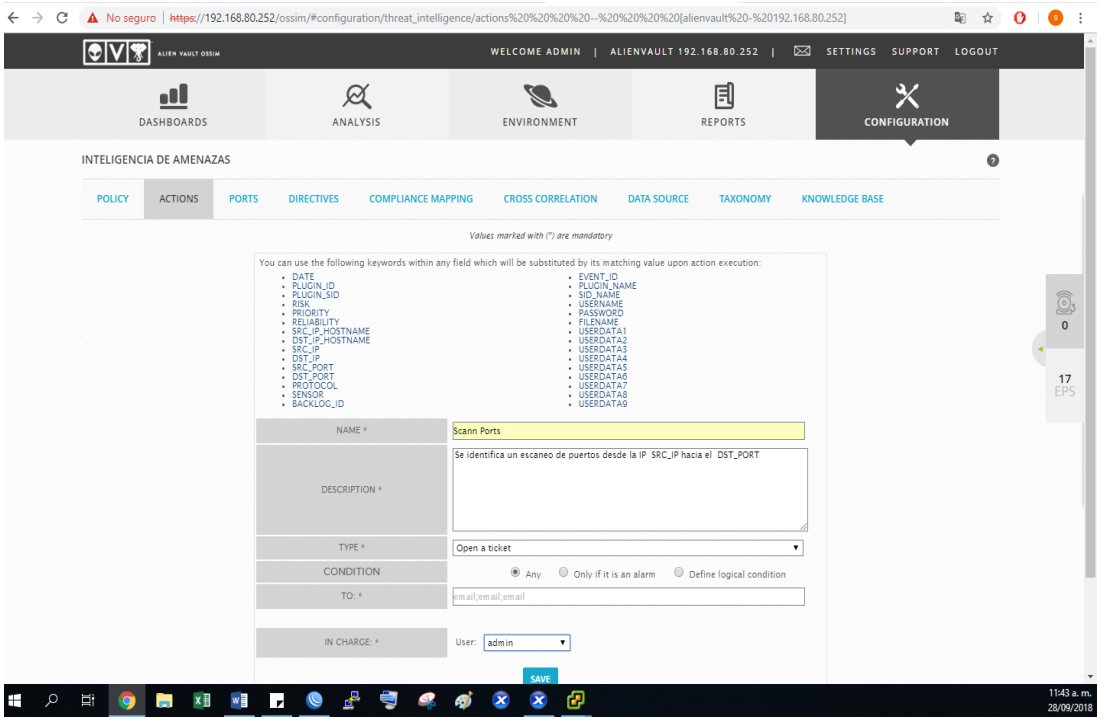


Ilustración 75. Acción para ataque Escaneo de puertos (Elaboración propia)

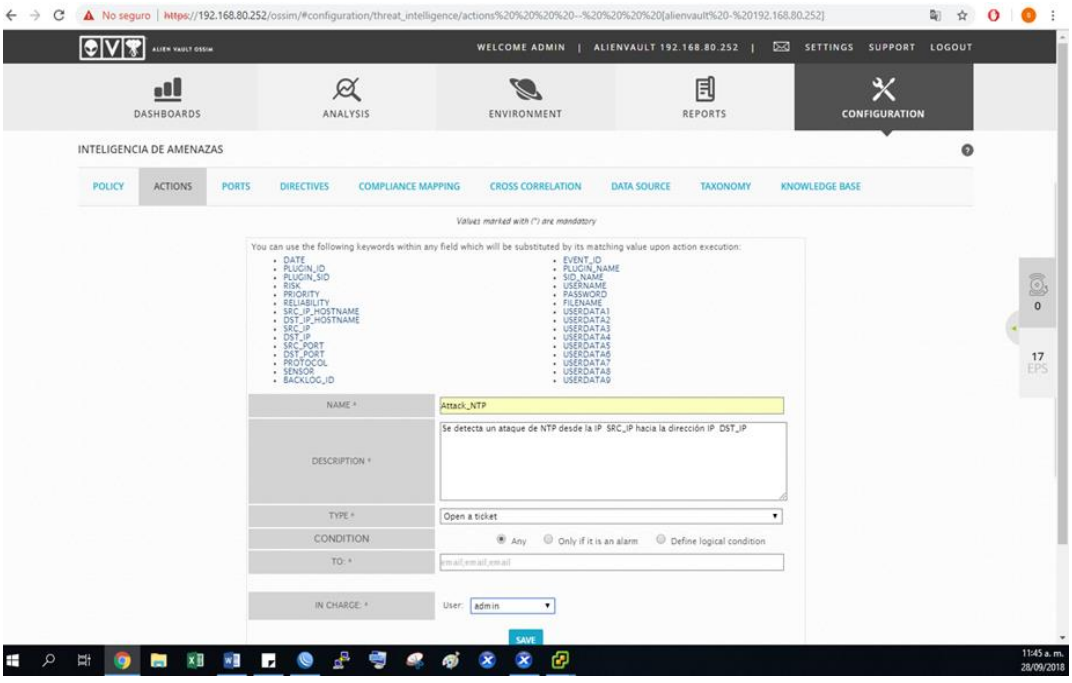


Ilustración 76. Acción para ataque NTP (Elaboración propia)

- **Configuración de reglas de correlación**

Inicialmente de para hacer la configuración de las reglas de correlación se hacen la sección de inteligencia de amenazas, como se muestra a continuación:

Escaneo de puertos

Ilustración 77. Nueva política (Elaboración propia)

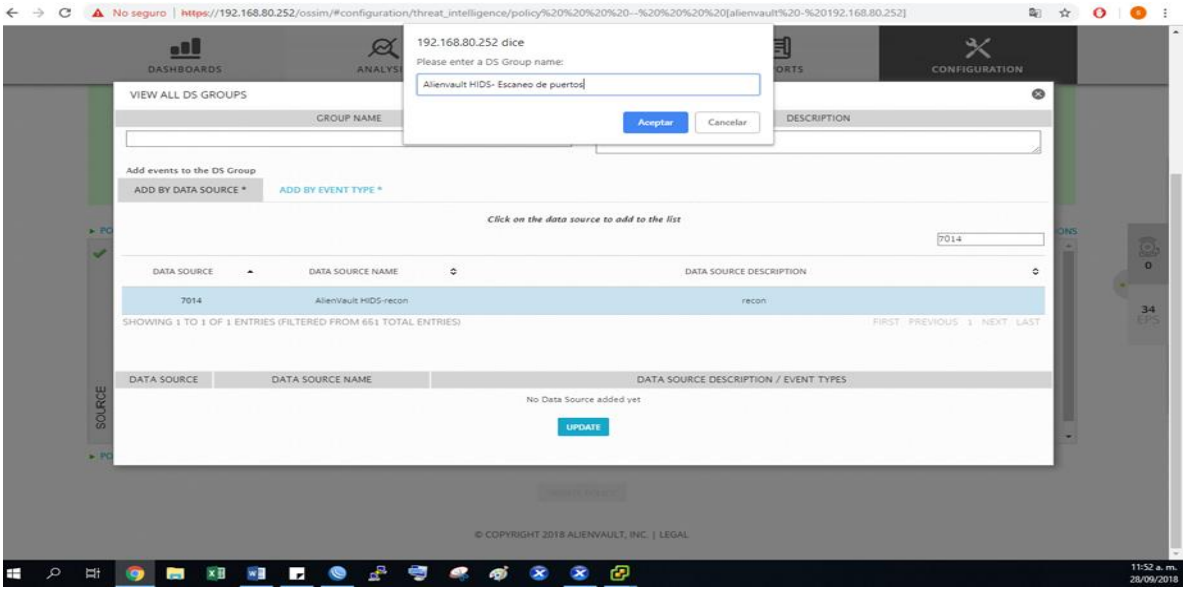


Ilustración 78. Plugin para regla de escaneo de puertos (Elaboración propia)

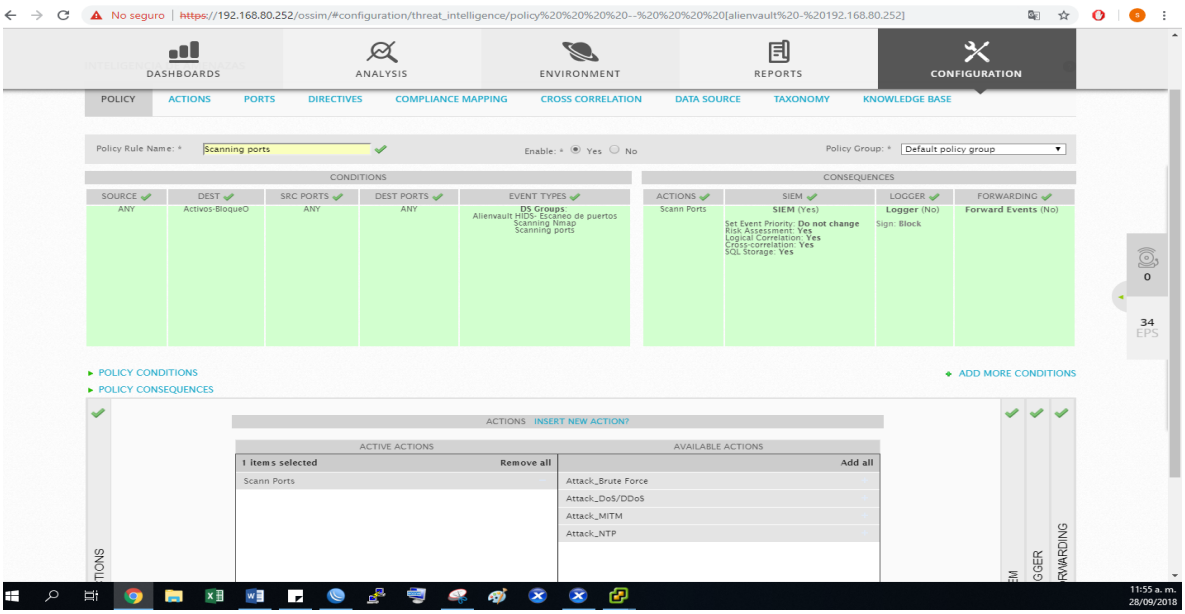


Ilustración 79. Regla de correlación para escaneo de puertos (Elaboración propia)

Denegación de servicio

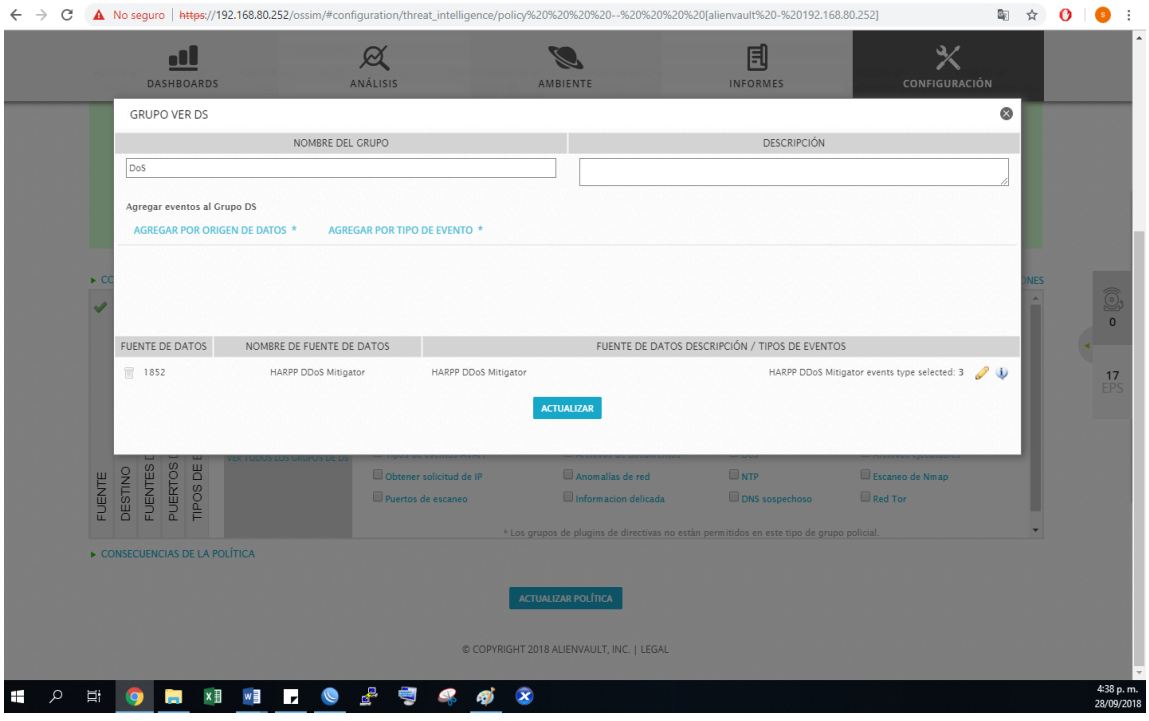


Ilustración 80. Plugin para regla denegación de servicio (Elaboración propia)

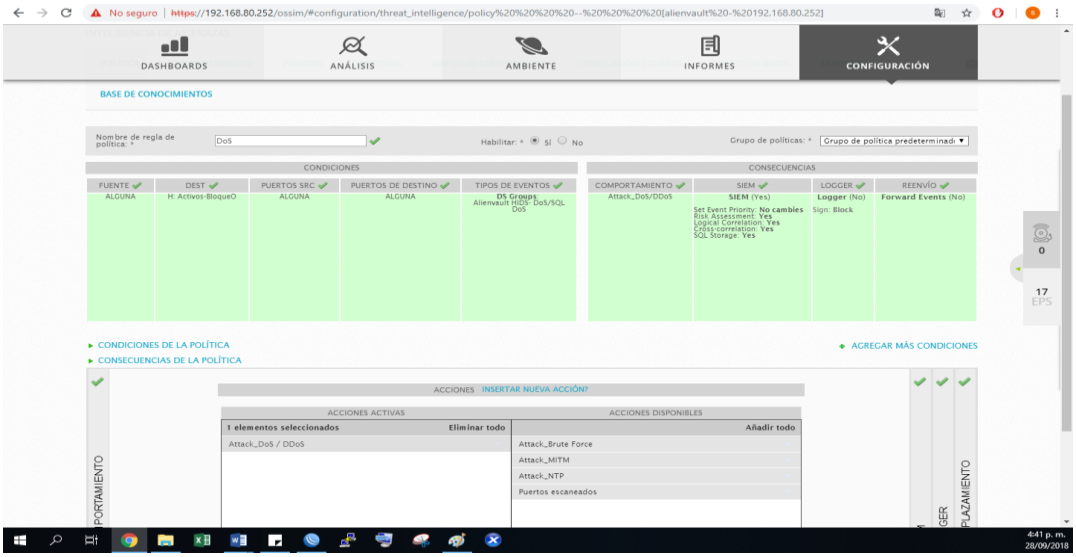


Ilustración 81. Regla de correlación para denegación de servicio (Elaboración propia)

Men In The Middle (MITM)

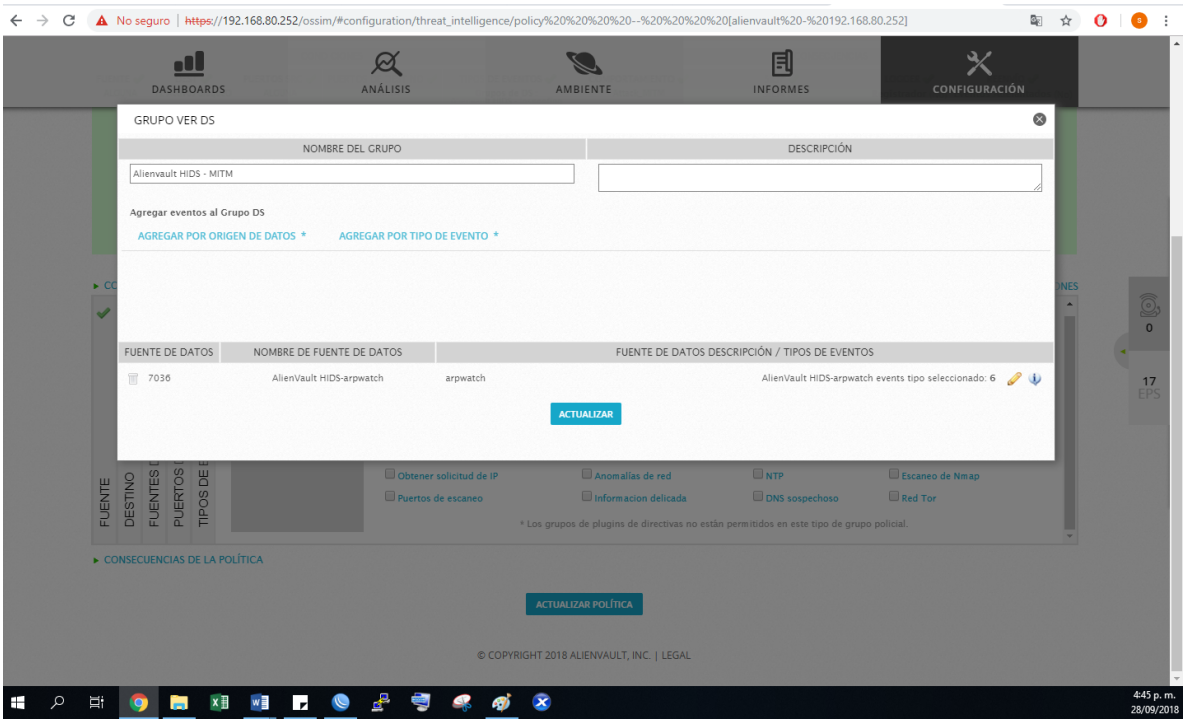


Ilustración 82. Plugin para regla MITM (Elaboración propia)

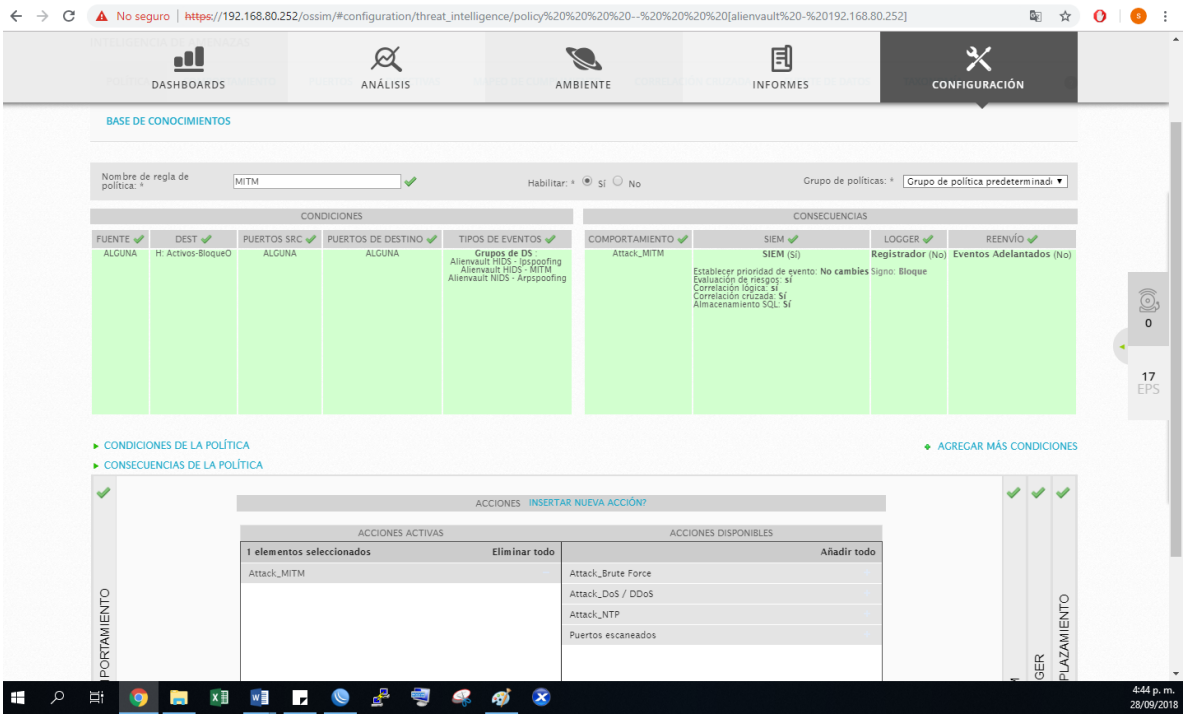


Ilustración 83.Regla de correlación para Men In The Middle (Elaboración propia)

Fuerza Bruta

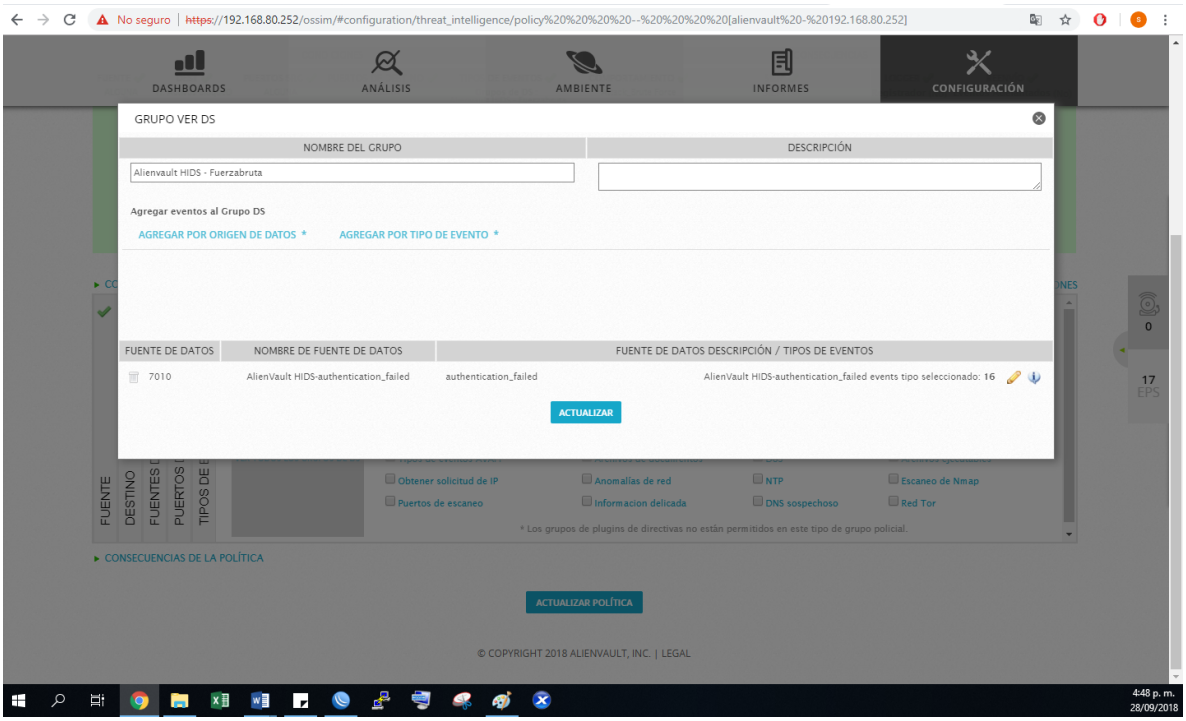


Ilustración 84. Plugin para regla de fuerza bruta (Elaboración propia)

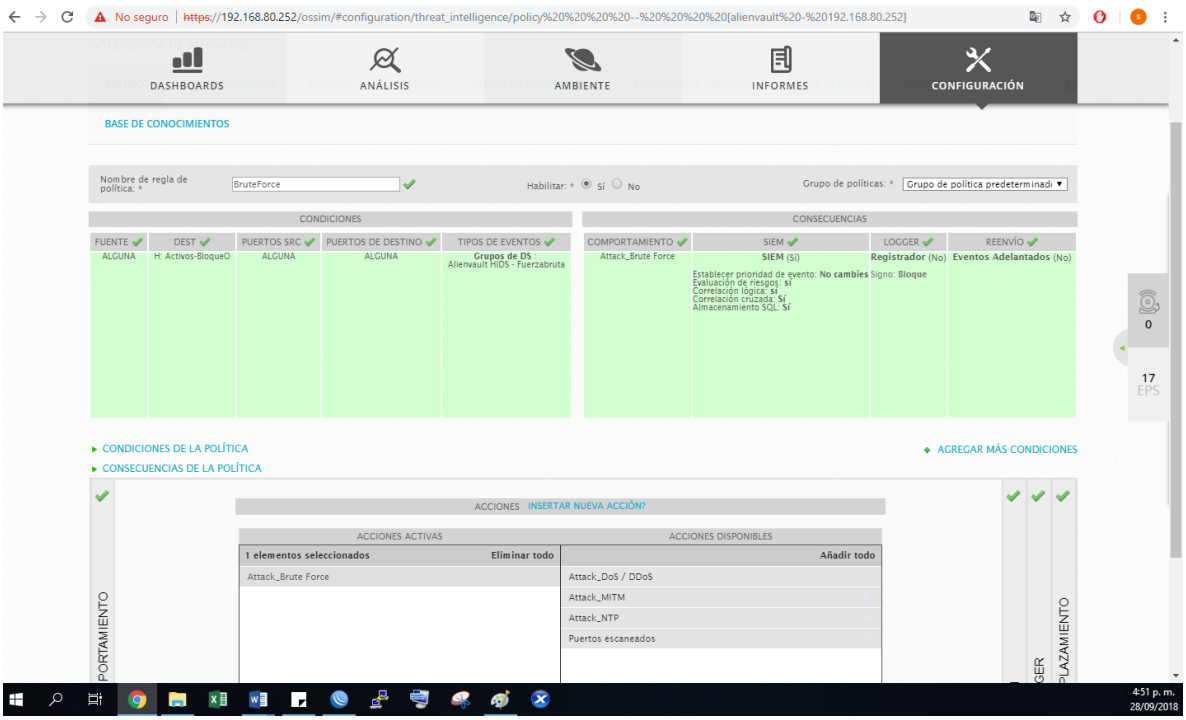


Ilustración 85. Regla de correlación para Fuerza bruta (Elaboración propia)

Network Time Protocol (NTP)

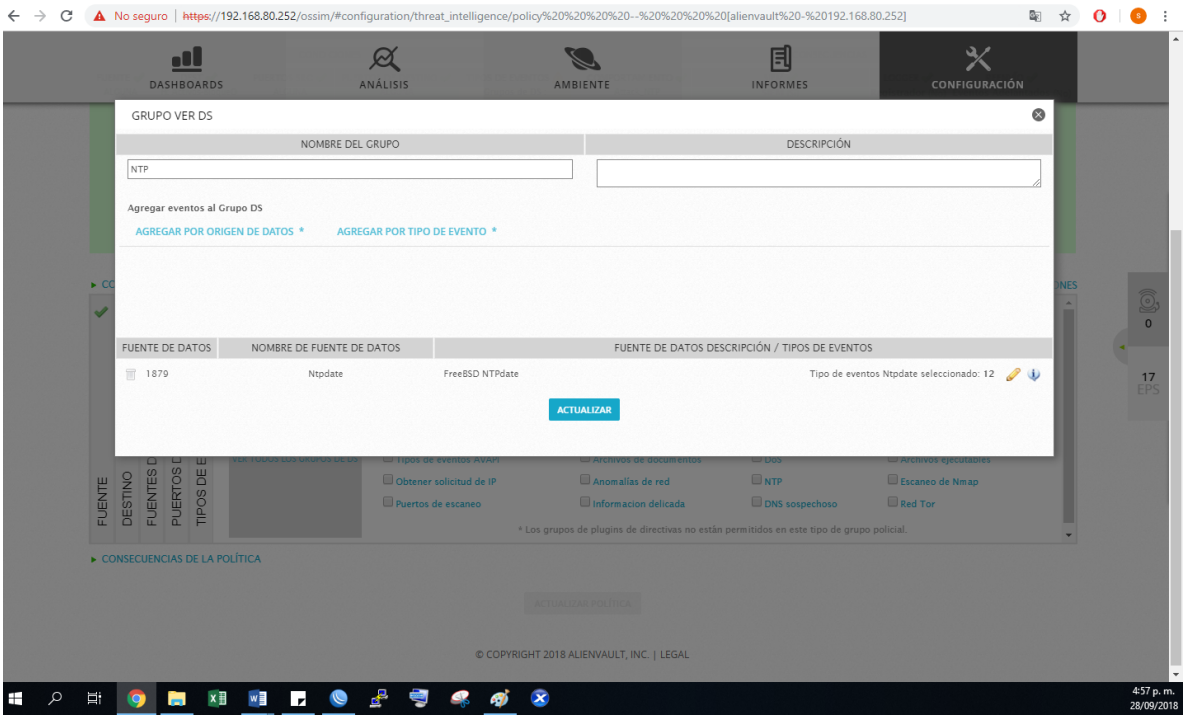


Ilustración 86.Plugin para regla de NTP (Elaboración propia)

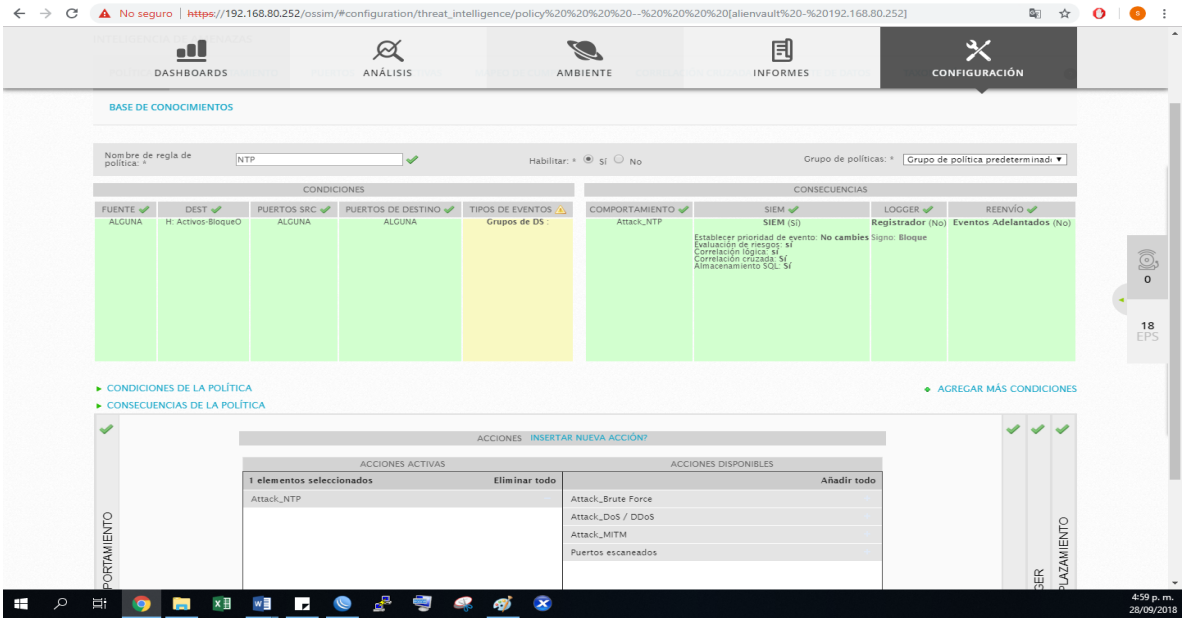


Ilustración 87. Regla de correlación para NTP (Elaboración propia)

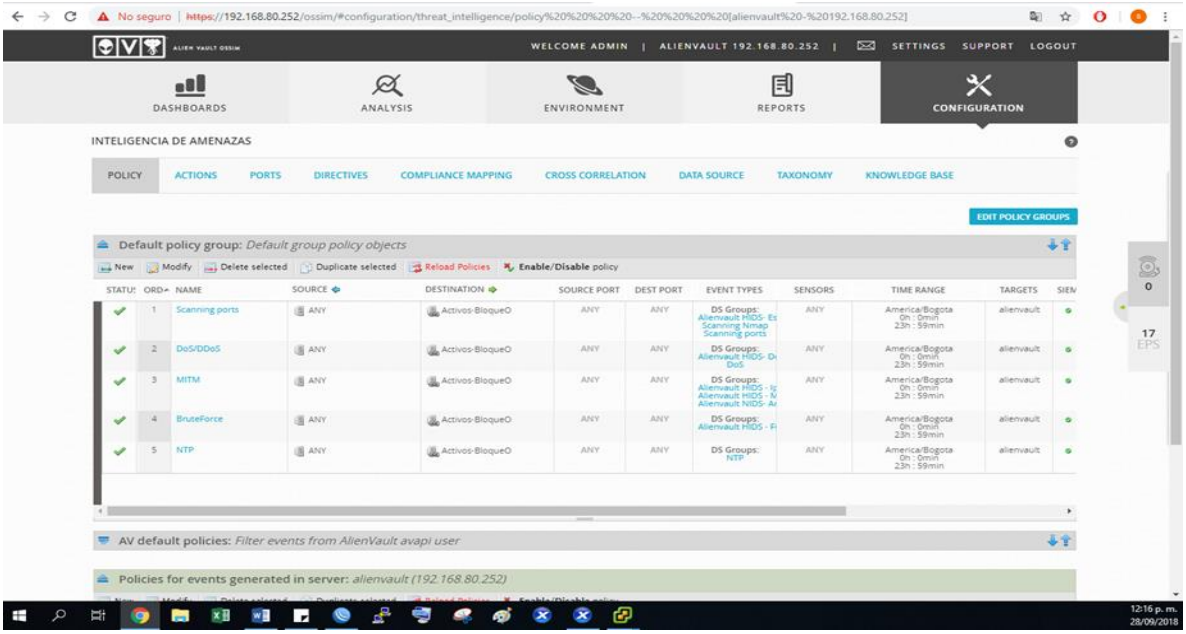


Ilustración 88. Reglas de correlación configuradas (Elaboración propia)

FIRMA ESTUDIANTES Sebastian Rivera Montoya

Carlos Alberto Pérez

FIRMA ASESOR Revisado y aprobado octubre 24/2018

FECHA ENTREGA:_____

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO___ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA:_____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA:_____