SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS IPS PARA LA VLAN DE SERVIDORES DE LA SOCIEDAD MINERA DE SANTANDER S.A.S. EN BUCARAMANGA (SANTANDER)

RAFAEL LUIS MOSCOTE MEDINA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BUCARAMANGA
2017

SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS IPS PARA LA VLAN DE SERVIDORES DE LA SOCIEDAD MINERA DE SANTANDER S.A.S. EN BUCARAMANGA (SANTANDER)

RAFAEL LUIS MOSCOTE MEDINA

Trabajo de grado para optar al título de Especialista en Seguridad Informática

Asesor
Jorge Enrique Ramírez Montañez
Ingeniero de Sistemas
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BUCARAMANGA
2017

Nota de aceptación

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bucaramanga, diciembre 12 de 2017.

DEDICATORIA

A Dios por darme sabiduría para asumir este reto, a mi hija Thaliana que es mi inspiración, a mi esposa por su compresión y apoyo, a mi mamá por su ejemplo de lucha incansable.

AGRADECIMIENTOS

A la Sociedad Minera de Santander S.A.S por facilitarme los recursos tecnológicos y brindarme todo el apoyo para el desarrollo de esta investigación, a Jorge Martinez (Asesor), gracias por todo el interés en el mejoramiento de la presentación y enfoque metodológico siguiendo los lineamientos de un proyecto, a Anderson Rivera (Gerente de TI) por su respaldo desde el momento que solicite el Aval para realizar este estudio, a mis compañeros que siempre me guiaron para que esta investigación avanzara, a la Universidad Nacional Abierta y a Distancia por esta oportunidad que brinda a los estudiantes a través de su metodología de aprendizaje autónomo, significativo y colaborativo, contribuyendo a la formación de profesionales con conocimientos sólidos en seguridad informática.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

Anomalía*:* No usual o desviado estadísticamente de lo normal.

Amenaza: Situación o evento con que puede provocar daños en un sistema.

Backdoors: por sus siglas en ingles puerta trasera, es una secuencia de códigos creada por el programador para acceder a la aplicación evadiendo la autenticación normal.

***Botnet*:** Hace referencia a una red robot informática que se ejecuta de manera autónoma o automática permite a los hackers tomar control de muchos equipos a la vez y convertirlos en equipos “Zombis”.

DMZ: conocida por sus siglas en inglés como Zona Desmilitarizada, es una zona segura que se ubica entre la red interna de una organización y una red externa para publicar servicios accesibles desde Internet.

DoS: es un ataque a un servidor o red (por sus siglas en ingles denegación de servicio) que causa que un servicio o recursos sea inaccesible para los usuarios legítimos.

Exploit: fragmentos de código o software para aprovechar una vulnerabilidad de seguridad de un sistema informático para conseguir un comportamiento no deseado del mismo.

Firewall: un cortafuego es una herramienta de seguridad informática que permite el filtrado de las conexiones entrantes y salientes en una red de datos.

HTTP: protocolo de transferencia de hipertexto.
ICMP: protocolo de mensajes de control de internet.
IPS: Sistema de prevención de intrusos (o por sus siglas en ingles IPS) es un tipo de software o hardware de seguridad informática que analiza el tráfico de la red en busca de patrones de ataques para bloquearlos.

IDS: Sistema de Detección de intrusos (o por sus siglas en ingles IDS) al contrario que el IPS estos sistemas solo detectan comportamientos anómalos en una red y alertan sobre ellos.

IP: por sus siglas en ingles Protocolo de Internet hace parte de la capa de red, permite el transporte de paquetes en una red sin garantizar su entrega.

Keylogger: es un tipo de software o dispositivo hardware especifico que se encarga de capturar las pulsaciones del teclado, para luego guardarlas en un archivo o enviarlas a través de internet.

Lipcap: librería utilizada para capturar paquetes en sistemas basados en Linux.

Malware: programa o software malicioso que tiene como objetivo infiltrarse o dañar un computador o sistema de información sin la autorización de sus propietarios.

Protocolo: con junto de reglas que rige el intercambio de información a través de una red de computadoras.

Sniffer: analizador de protocolos que captura las tramas de una red de datos.

TCP: protocolo de control de transmisión, es uno de los protocolos fundamentales de internet.

Software libre: aplicación desarrollada para libre distribución con licencia GPL.

UDP: protocolo de la capa de transporte basado en datagramas.

VLAN: por sus siglas en ingles Red de Área Local Virtual, es un método para crear redes lógicas dentro de una misma red física.

Vulnerabilidad: las vulnerabilidades son brechas o agujeros en los sistemas o redes que son aprovechadas para violar las políticas de seguridad.

INTRODUCCION

Con la creciente demanda de los servicios en Internet y la computación en la nube, la mayoría de las empresas han decidido migrar sus sistemas y aplicaciones a esta nueva plataforma, no solo por las ventajas que les ofrece, sino también por los grandes ahorros en infraestructura tecnológica que representa para el negocio. Al mismo tiempo, la seguridad informática se ha convertido en uno de los principales pilares que las compañías han venido adoptando para protegerse de las amenazas y ataques. Como consecuencia, ha permitido el auge de sofisticadas técnicas de intrusiones que buscan vulnerar los sistemas informáticos de una manera silenciosa aprovechando el tiempo que estas tardan en ser detectas. Por esta razón, es importante que las compañías implementen sistemas de seguridad robustos en sus redes y sistemas informáticos, por los riesgos que puede representar la pérdida o robo de información sensible. Cabe destacar, que los sistemas de detección y prevención de intrusos se han vuelto indispensable en este sentido, dado que estos realizan un monitoreo de la red en tiempo real utilizando técnicas basadas en firmas para identificar patrones de ataques y su bloqueo inmediato. Estos sistemas resultan muy eficaces por su capacidad de detectar y alertar de posibles intrusiones en sus primeras fases y ayudan a mejorar el ancho de banda y estabilidad de la red.

A continuación, se describe el desarrollo y metodología empleada en el proyecto aplicado “Sistema de Detección y Prevención de Intrusos *IPS* para La Vlan De Servidores de La Sociedad Minera de Santander S.A.S. en Bucaramanga (Santander)”, inicialmente se explica los método y técnicas que se utilizaron para el levantamiento de información del esquema de seguridad actual de la red de datos y luego se realizó un análisis que permitió desde el planteamiento del problema conocer los síntomas y causas de los ataques informáticos que hoy por hoy están afectando a las empresas a nivel mundial, se establecen uno objetivos y se define

una metodología de investigación para buscar soluciones a los intentos de acceso no autorizados a que puede estar expuesto el segmento de red de los servidores de Minesa S.A.S, a través de la instalación de un sistema de detección y prevención de intrusos que monitorea el tráfico de la red en tiempo real para detectar y bloquear ataques de manera automática.

1. TITULO

SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS IPS PARA LA VLAN DE SERVIDORES DE LA SOCIEDAD MINERA DE SANTANDER S.A.S. EN BUCARAMANGA (SANTANDER)

2. PLANTEAMIENTO DEL PROBLEMA

Los numerosos ataques que a diario se registran en las redes de datos a nivel mundial, ya sea por fugas de información, denegación de servicios e interceptación de tráfico y que muchas veces nos son detectados por los *firewalls* o dispositivos de seguridad, son una muestra más de las falencias que hoy en día presentan las empresas en materia de seguridad. Según el reporte de Seguridad por ESET del 2015[1], los incidentes que sufrieron las empresas latinoamericanas en el 2014 fueron: accesos indebidos, infección por *malware* y ataques de denegación de servicio *DoS*. En Colombia en un 10% crecieron las amenazas de *Botnets* durante el 2014. Lo anterior, ha despertado un gran interés en el conocimiento de las nuevas técnicas y mecanismos que permitan detectar estas intrusiones en tiempo real.

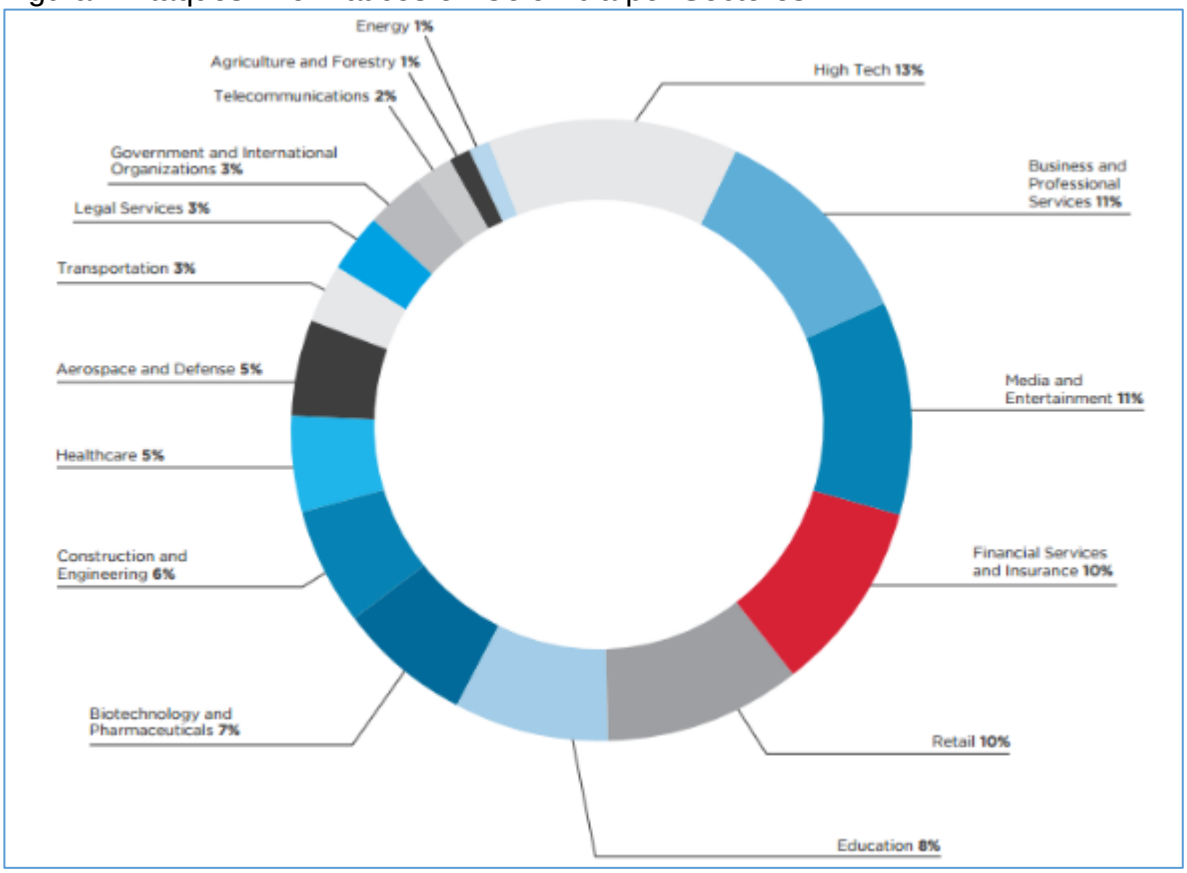
En los últimos años el 98% de empresas colombianas han sido víctimas de ataques informáticos[2], según FireEye Inc empresa líder en detección de ataques cibernéticos, muchos de ellos no son detectados por los administradores de la plataforma de red, debido a la falta de conocimiento de la misma o inadecuada configuración de los equipos de protección. La Figura 1 muestra los sectores más afectados por estos ataques los cuales son: gobierno, servicios, consultoría y financiero. Cabe destacar que las principales fuentes de ataques son vía web e Email. El sector Financiero y Seguros han sido los más afectados por estos ataques. Por lo contrario, el de energía es el que menos ataques ha recibido.

---

[1] ESET. (7 de enero de 2015). ESET Security Report 2015. Recuperado el 30 de septiembre de 2017, de ESET: https://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf

2 Ataques informáticos en Colombia y sectores más afectados. (11 de Marzo de 2014). Recuperado el 30 de Agosto de 2016, de http://www.vanguardia.com/actualidad/colombia/250540-98-de-empresas-colombianas-son-victimas-de-ataques-informaticos

Figura 1 Ataques Informáticos en Colombia por Sectores



Fuente: https://www.fireeye.com/

A pesar de esto, las empresas por ahorro de costos de implementación y mantenimiento en sus infraestructuras y por los beneficios que ofrece la computación en la nube deciden migrar sus plataformas a estos entornos, exponiendo sus datos. Sin embargo, descuidan muchos aspectos de seguridad que sin lugar a duda pueden comprometer unos de sus activos más importantes que es la información.

No obstante, un inadecuado diseño en su esquema de seguridad puede generar brechas que los intrusos pueden aprovechar para rastrear a sus víctimas colocando en riesgo sus datos. Es necesario realizar un estudio del esquema de seguridad

actual en la Red de Área Local Virtual (*VLAN*) de servidores de la empresa Minesa S.A.S y proponer alternativas que, combinadas al sistema existente, permitan detectar en tiempo real la presencia de intrusos o comportamientos anómalos en el tráfico de esta red.

2.1 FORMULACION DEL PROBLEMA

¿Cómo desarrollar la capacidad para detectar la presencia de intrusos en tiempo real, en la *VLAN* de servidores de la Sociedad Minera de Santander S.A.S a partir de análisis de la arquitectura de red actual para encontrar vulnerabilidades?

3. JUSTIFICACION

Minesa S.A.S es un proyecto de Minería de oro en Colombia que se encuentra en la fase de aprobación de los estudios de impacto ambiental para obtener la licencia ambiental y dar inicio a la explotación, cuenta con una sede principal ubicada en la ciudad de Bucaramanga y sucursales en la ciudad de Bogotá D.C, y municipio de California (Santander); que es la sede base de sus operaciones. Actualmente se encuentra reestructurando su departamento de tecnología y entre sus prioridades la definir un esquema de seguridad que garantice la disponibilidad, integridad y confidencialidad de su información, para ello la Gerencia de Tecnología se encuentra definiendo los procedimientos, normas y políticas de seguridad de la información. Recientemente se implementó un sistema de seguridad de última tecnología que le permite detectar y prevenir de forma anticipada intrusos en su red de datos.

El sistema de seguridad perimetral actual realiza un filtrado de todas las conexiones entrantes y salientes, con capacidades de prevención de intrusos tanto en su red interna y externa. Sin embargo, se ha comprobado que la mayoría de los ataques que se presentan en una red de datos son a nivel interno. Por ello es importante que se realice un estudio del esquema de seguridad actual para identificar a nivel de la red local como se puede proteger la empresa de ataques internos, este proyecto busca fortalecer las capacidades de detección y protección del segmento de red de sus servidores, a través de un monitoreo del tráfico que ingresa a la red en tiempo real, que permita detectar comportamientos anómalos e intrusiones, entre los beneficios que aportará está el del mejoramiento del consumo del ancho de banda al poder descartar paquetes no deseados o la prevención de ataques en sus primeras fases.

Proyectos similares se han implantado en muchas organizaciones a nivel mundial, como referencia está el de la Universidad de Valencia en España, se implementó un sistema de detección de intrusos como herramienta para facilitar a los administradores la detección de ataques en la red. Por consiguiente, se logró identificar que la Universidad recibe en promedio diario seis (6) ataques tipo *exploit*[3]. Desde el punto de vista comercial, la implementación de un *IPS* resulta costoso, existen muchas alternativas a nivel de software libre con respaldo de comunidades que mantienen día a día actualizaciones de nuevos ataques, lo que hace el proyecto viable desde el punto de vista económico y técnico y que se pueda implementar con recursos actuales, dado que no se requiere inversión en licenciamiento de *software* y *hardware*.

[3] MIRA ALFARO, Emilio José, Implantación de un sistema de detección de intrusos en la Universidad de Valencia. España. 2012. 142 p.

4. OBJETIVOS DEL PROYECTO

4.1 OBJETIVO GENERAL

Instalar un sistema de detección y prevención de intrusos, utilizando la arquitectura del *Snort*, como mecanismo para fortalecer la seguridad en la *VLAN* de servidores de la Sociedad Minera de Santander S.A.S. en Bucaramanga (Santander).

4.2 OBJETIVOS ESPECÍFICOS

- Recopilar información del esquema de seguridad de la *VLAN* de servidores de la Empresa Minesa S.A.S, utilizando técnicas de recolección de datos para conocer el nivel de protección.

- Diseñar un esquema de red utilizando *IPS* detrás del firewall que permita monitorear el tráfico que entra a la *VLAN* de servidores para detectar intentos de ataque y fortalecer la seguridad de la red local de la Empresa Minesa S.A.S

- Instalar el sistema de seguridad con la herramienta *IPS* para bloquear las vulnerabilidades y amenazas que presenta *VLAN* de servidores de la Empresa Minesa S.A.S

5. MARCO DE REFERENCIA

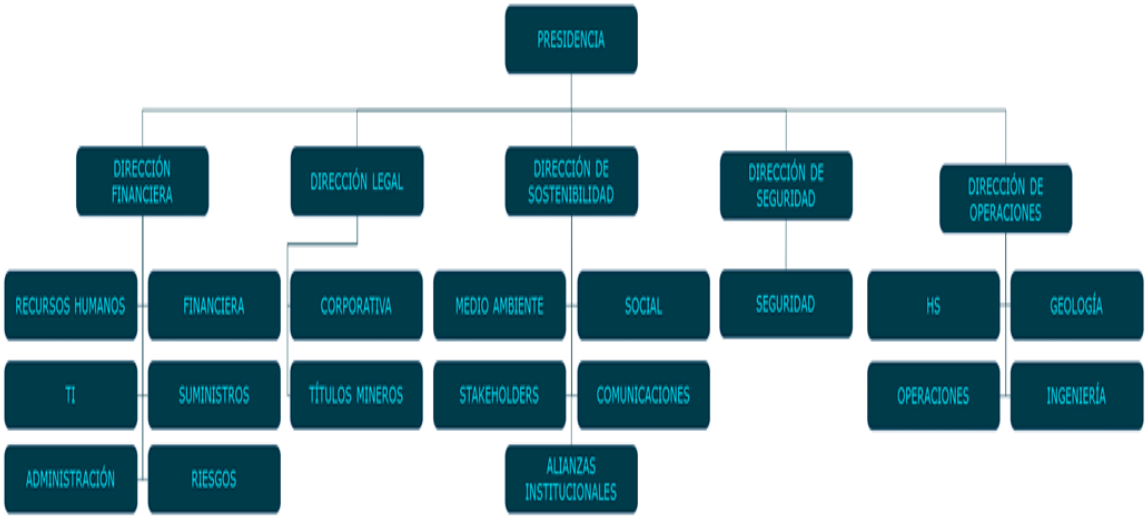
5.1 MARCO CONTEXTUAL

La Sociedad Minera de Santander S.A.S, Minesa, es una compañía de oro colombiana enfocada en el desarrollo de una operación minera basada en los más altos estándares de salud ocupacional, seguridad industrial y manejo ambiental.
El proyecto Soto Norte de Minesa está localizado en los municipios de California y Suratá en el departamento de Santander. Es una de las reservas de oro sin desarrollar más importantes de Suramérica.[4]

[4] Sitio Web Sociedad Minera de Santander S.A.S. (15 de noviembre de 2015). Recuperado el 30 de agosto de 2016, de http://www.minesa.com

5.1.1 Organigrama

Figura 2 Organigrama Estructura Organizacional Minesa



Fuente: http://www.minesa.com/quienes-somos/equipo-corporativo/

5.1.2 Misión

- Protegemos nuestro medio ambiente.

- Mejoramos las vidas de nuestros empleados y la comunidad generando desarrollo para Santander y Colombia.

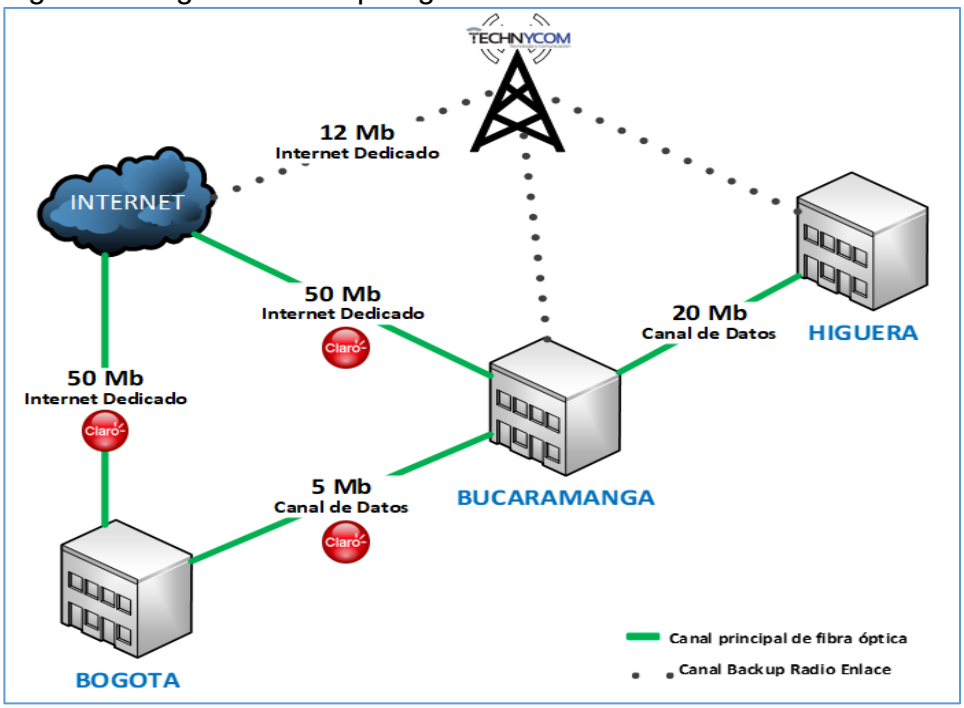
- Usamos la última tecnología y sistemas de gestión para una operación minera segura, eficiente y rentable.[5]

[5] Sitio Web Sociedad Minera de Santander S.A.S. (15 de noviembre de 2015). Recuperado el 30 de agosto de 2016, de http://minesa.com/es/who-we-are/mission-and-vision/

5.1.3 Visión. La compañía Líder en Minería de Oro más admirada en Colombia.[6]

5.1.4 Diagrama de Topología de Red de Minesa S.A.S. La Figura 3 muestra la topología de red de datos actual, conformada por canales de internet dedicado de 50 MB para la sede de Bogotá y Bucaramanga respectivamente. También, cuenta con un canal de datos de 20 MB que enlaza la Oficina de Bucaramanga y La Higuera (Campamento de Operaciones), 5 MB para el canal entre Bogotá y Bucaramanga. El servicio de Internet principal es prestado por el proveedor Claro a través de Fibra Óptica y el de contingencia por Technycom utilizando enlaces microondas.

Figura 3 Diagrama de Topología de Red de Minesa S.A.S



Fuente: Documentación Departamento TI Minesa

[6] Sitio Web Sociedad Minera de Santander S.A.S. (15 de noviembre de 2015). Recuperado el 30 de agosto de 2016, de http://minesa.com/es/who-we-are/mission-and-vision/http://minesa.com/es/who-we-are/mission-and-visio/

5.2 MARCO HISTORICO

En los años Ochenta James P. Anderson realizó un estudio sobre la seguridad en los sistemas de informáticos que utilizaban las Fuerzas Aéreas de los Estados Unidos, se trataba de un análisis de eventos en los computadores, la cual era una tarea que era muy tediosa llevarla manualmente y se debía automatizar, dado que era imposible analizar los millones de registros generados a diario en estos equipos, lo que hacía más difícil el descubrimiento y detección de anomalías por los auditores[7]. Lo anterior dio origen al primer sistema de detección de intrusos, el cual permitía auditar aquellos accesos a los computadores que no eran autorizados. El propósito de estos sistemas era el de eliminar información redundante en los eventos registrados, diferenciando los ataques internos de los externos basado en los patrones de comportamientos normales de los usuarios, que luego eran comparados en tiempo real para alertar de posibles ataques o desviaciones. Poco a poco fueron apareciendo numerosos sistemas de detección de intrusos entre los que se destacaron los siguientes:

- El IDES o "*Intrusión Detection Expert System*", este sistema funcionaba en tiempo real y era capaz de detectar anomalías o intentos de acceso no autorizados, utilizaba un sistema experto con el que evitaba la evasión de los intrusos.

- En 1990 se creó el *Distributed Intrusion Detection System (DIDS),* como la primera fusión que se hace entre sistemas de detección de intrusos basados en host y red, al principio presentó grandes dificultades al momento de registrar eventos asociados a distintas máquinas de la red.

[7] GONZALEZ GOMEZ, Diego, Sistemas de Detección de Intrusiones, p.7

- El *Multics Intrusion Detection and Alerting System (MIDAS)* se convirtió en uno de los primeros sistemas de detección de intrusos conectados a Internet, basado en detección de anomalías y reglas.

5.3 ANTECEDENTES

5.3.1 Sistema de Prevención de Intrusos para mejorar la seguridad de los servidores de la Universidad Nacional de Trujillo. Este sistema fue desarrollado para mejorar la seguridad de los servidores de la Universidad Nacional de Trujillo[8] basado en software libre, el cual permite detectar en tiempo real los posibles intentos de accesos no autorizados a los servidores, estas reglas eran aplicadas de acuerdo con las necesidades de la oficina de sistemas e Informática. El proyecto de investigación fue sobre un sistema de prevención de intrusos basado en host que se encargaba de monitorear todos los eventos en los servidores de la Universidad.

5.3.2 Implementación de un sistema de detección de intrusos (IDS) en la Dirección General de la Sede Central del Instituto Nacional Penitenciario y Carcelario INPEC "PIDSINPEC". El Proyecto estaba orientado a la implementación de un IDS en la Sede Central del INPEC, como medida de prevención de intrusos en red, con capacidad de generar alertas al detectar la presencia de algún tráfico anómalo, estas luego eran almacenadas en una base de datos que registraba los tipos de vulnerabilidades encontradas, este sistema utilizó la arquitectura del Snort en ambiente *Windows*[9].

[8] Sistema de Prevención de Intrusos Universidad Nacional de Trujillo. (noviembre de 2014). Recuperado el 18 de octubre de 2016, de http://www.inf.unitru.edu.pe/revistas/2014/6.pdf
[9] Sistema de detección de intrusos (IDS) del INPEC. (7 de Mayo de 2015). Recuperado el 10 de Octubre de 2016, de http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3494/3/86057594.pdf

5.3.3 Implantación de un sistema de Detección de Intrusos en la Universidad de Valencia. Sistema de detección de intrusos con capacidad de generar un informe diario de todas las alertas de tráfico inusual que es enviado de manera automática a través de email al administrador de seguridad y de esta manera activar los planes de contingencia evitando que estos agujeros de seguridad impacten los sistemas informáticos de la Universidad, el *IDS* es basado en red con ubicaciones antes y después del firewall que analizaba el tráfico que no detectaba el cortafuego[10].

5.3.4 Sistema Preventor de Intrusos para la Esime Zacatenco. Sistema que permitió obtener registros de toda actividad mal intencionada en la red de datos de La Estime y Zacatenco, se realizaron pruebas de bloqueos de ataques, infecciones con virus e intento de accesos indebidos, se instaló con Snort en modo IPS bajo el sistema operativo *Linux*[11].

5.4 MARCO TEORICO

Para el desarrollo de la presente investigación fue necesario estudiar el componente teórico de un sistema de detección de intrusos al mismo tiempo que su evolución a un *IPS*. También, sus características principales, arquitectura, funcionamiento y los tipos de sistemas de detección de intrusos existentes. También, se utilizó el modelo *OSI* como referencia para identificar la capa de red donde se capturan los paquetes que luego son procesados y pasados al motor de detección para generar las alertas causadas por las anomalías encontradas en los protocolos.

[10] Implantación de un sistema de Detección de Intrusos en la Universidad de Valencia. (15 de octubre de 2016). Obtenido de http://www.rediris.es/cert/doc/pdf/ids-uv.pdf
[11] Sistema de Prevención de Intrusos Universidad Nacional de Trujillo. (16 de octubre de 2016). Obtenido de http://www.inf.unitru.edu.pe/revistas/2014/6.pdf

5.4.1 Sistema de Detección de Intrusos (IDS). Sistema que monitorea el tráfico en una red, capaz de detectar códigos maliciosos en las cabeceras de los paquetes que pueden pasar desapercibidos a través de los puertos filtrados en los cortafuegos, encargados de generar alertas en tiempo real, utilizan el lenguaje de reglas para analizar los protocolos de la capa de red y detectar anomalías por medio de alertas. En efecto son útiles cuando se ubican en distintos puntos de la red, porque ayudan a mejorar errores en las configuraciones y vulnerabilidades. Los *IPS* a diferencia del *Firewall* los bloqueos no los realizan a nivel de puerto y direcciones *IP*, por el contrario, el análisis lo hacen a nivel de protocolos, capaces de bloquear ataques. Los Sistemas de Detección de Intrusos también se clasifican por la función que ejercen frente a un ataque los hay de dos tipos [12]:

- Reacción: supervisa los logs del sistema, cuando detecta una anomalía genera la alerta.

- Prevención: Escanea constantemente el tráfico de la red (*Sniffer*), si detecta paquetes en tránsito anómalos actúa[13].

5.4.1.1 Ventajas

- Detección anticipada de ataques y envío de alertas a los administradores para que se activen los planes de contingencia.

- Análisis de protocolos en los paquetes que son filtrados por el *firewall.*

- Fácil instalación, configuración y administración.

[12] Sistema de detección de intrusos. (2005). Recuperado el 20 de Octubre de 2016, de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html
[13] SALAZAR MORALES, Jorge, Seguridad Avanzada en Redes de Datos. Medellín. 2015 144 p.

5.4.1.2 Características

- Capacidad de reacción automática ante la detección de un ataque.
- Aplicación de nuevos filtros conforme detecta ataques en progreso.
- Mínima vigilancia.
- Disminución de falsas positivos de ataques a la red.
- Bloqueo automático de ataques ocurridos en tiempo real.
- Protección de sistemas no parchados.
- Optimización en el rendimiento del tráfico de la red.

5.4.1.3 Clasificación. Los sistemas de prevención de intrusiones se pueden clasificar en cuatro tipos diferentes:

1. *Prevention Intrusion Network (PIN):* Basado en la red detectan tráfico sospechoso, mediante el análisis de la actividad de protocolo.

2. *Wireless Intrusion Prevention System (WIPS):* Sistemas de prevención de intrusiones inalámbricas, detectan tráfico malicioso mediante el análisis de protocolos de redes inalámbricas.

3. *Network Behavior Analysis (NBA):* Análisis de comportamiento de la red, examina el tráfico para identificar las amenazas que generan flujos de tráfico

inusuales, como escaneo de red, denegación de servicios, ciertas formas de malware y violaciones de política.

4. *Host-based Intrusion Prevention System (HIPS):* Los sistemas de prevención de intrusos basados en host controlan y detectan actividades sospechosas como acceso no autorizado y cambios en la configuración en el equipo que monitorean.

5.4.1.4 Métodos de Detección. La mayoría de los sistemas de prevención de intrusos utilizan uno de los tres (3) métodos de detección que son: basados en firmas, anomalías estadísticas basadas en el protocolo y el análisis de estado.

1. Detección basada en firmas: Este método de detección utiliza reglas basada en patrones de ataque que se comparan con el paquete capturado y si cumple con los parámetros de inmediato es bloqueado.

2. Anomalía basada en estadísticas de detección: Mediante este método los *IPS* crean una línea base que representa la actividad normal de los usuarios, generalmente cuando existe un ataque el sistema detecta un desvío del comportamiento normal de la red y genera la acción.

3. De estado de detección de análisis de protocolo: Este método identifica anomalías en protocolo comparando los encabezados de los paquetes y tomando la acción si no cumple con los parámetros que lo identifican[14].

[14] Módulo de Seguridad Informática. (30 de agosto de 2016). Obtenido de http://www.cybsec.com/upload/ESPE_IDS_vs_IPS.pdf

Existen en el mercado muchas clases de *IPS* destacando se entre ellos: los *Cisco NetRanger*, *Omniguard Intruder Alert*, *Polycenter Security Intrusion Detector* y *Dragon* entre otros. Otros de los IPS Software libre que se destacan el *Shadow*, *Suricata*, *Snort* y *Tripwire*.

5.4.2 El Modelo de Referencia OSI. El modelo de referencia *OSI* es otro de los componentes teóricos relacionados con el Sistema de Prevención de Intrusos, como este funciona en red se hace necesario conocer cada una de las capas que lo conforman, en la capa de enlace es donde ocurre la captura el tráfico por el módulo de adquisición y que luego es decodificada por el preprocesador y entregada al motor de detección que se encarga de comparar con las reglas y luego tomar la acción de descartar o permitir el paso del paquete a la siguiente capa. Cada una de ellas cumple una función específica que es requerida para comprender la ruta de los paquetes que son analizados por el sistema de prevención de intrusos. A continuación, se describen las siete (7) capas del modelo de referencia:

- Capa de Aplicación: es la capa siete (7) del modelo OSI con mayor interacción por el usuario; proporciona servicios de red a las diferentes aplicaciones del usuario. Difiere de las demás capas debido a que no suministra servicios a ninguna otra capa *OSI*. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo y navegadores de internet entre otros.

- Capa Presentación: conocida como la capa seis (6) garantiza que la información que envía la capa de aplicación sea interpretada por su equivalente en el destino.

- Capa de Sesión: capa cinco (5), establece, administra y termina las sesiones entre dos hosts que se están comunicando. La capa de sesión brinda servicios

a la capa de presentación. También sincroniza el diálogo entre las capas de presentación en una conexión y administra su intercambio de datos.

- Capa Transporte: la capa cuatro (4) segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro primeras capas se encargan del transporte de datos.

- Capa de Red: la capa tres (3) proporciona conectividad y selección de ruta entre dos equipos para el envío y recepción de información que pueden estar en diferentes ubicaciones geográficamente.

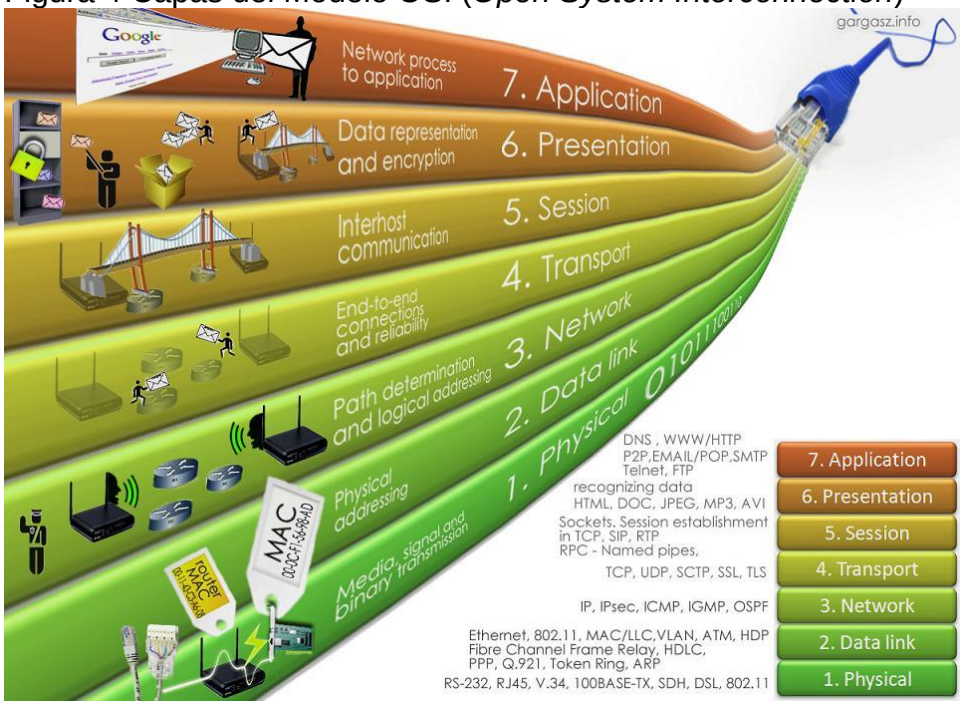
- Capa de Enlace: la capa dos (2) se encarga del establecimiento de una comunicación segura entre dos hosts pertenecientes a la misma red o subred, entre las funciones que cumple se destaca el flujo y la transmisión de datos libre de errores.

- Capa Física: la capa uno (1) define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales[15].

La Figura 4 muestra el modelo de referencia *OSI* que es el estándar utilizado para representar la ruta que siguen los paquetes en una comunicación antes de llegar el destino y como ocurre todo el proceso de codificación y decodificación en cada una de las capas por medio de los protocolos que la integran.

[15] Modelo OSI. (25 de Octubre de 2016). Obtenido de http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

Figura 4 Capas del Modelo OSI (*Open System Interconnection*)



Fuente: http://gargasz.info/wp-content/uploads/2010/01/OSI_model_LAN.jpg

5.5 MARCO CONCEPTUAL

- Seguridad de la Información: Es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información[16]

- Seguridad Informática: Es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida[17]

[16] ESCRIVÁ GASCÓ, Gema, Seguridad Informática, p.7
[17] ESCRIVÁ Op. cit., p.7.

- Seguridad física: Se asocia a la protección física del sistema ante amenazas como inundaciones, incendios, robos entre otros[18].

- Seguridad lógica: Mecanismo que protege la parte lógica de un sistema informático (Datos, aplicaciones y sistemas operativos). Uno de los medios más utilizado es la criptografía[19].

- Amenaza: Es cualquier evento accidental o intencionado que puede ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo de la organización[20].

- Vulnerabilidad: Es cualquier debilidad en el sistema operativo que pueda permitir a las amenazas causarle daños y producir perdidas a la organización[21].

- Ataque: Es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre alguna vulnerabilidad y tener control total del mismo[22]. Las etapas de un ataque según los autores de libro de la administración de los sistemas operativo son[23]:

1. Recogida de Información.

2. Ataque inicial.

3. Acceso completo al sistema.

---

[18] ESCRIVÁ Op. cit., p.7.
[19] ESCRIVÁ Op. cit., p.7.
[20] ESCRIVÁ Op. cit., p.7.
[21] ESCRIVÁ Op. cit., p.7.
[22] ESCRIVÁ Op. cit., p.7.
[23] COLOBRAN HUGUET, Miquel, ARQUÉS SOLDEVILLA, Josep María, MARCO GALINDO, Eduard, Administracion de Sistemas Operativos en Red, p. 229

4. Instalación de *backdoors*, *keylogger* y troyanos para obtener información y asegurar futuros acceso del atacante.

5. Eliminación de huellas.

- Intruso: Es una de las dos amenazas más extendidas la otra son los virus, generalmente es conocido como *hacker* o *cracker*[24].

- Puerta Trasera: Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar “atajos” en los sistemas habituales de autenticación del programa o código que se está diseñando[25].

- Falso positivo: También se conoce como falsa alarma y corresponde a tráfico inofensivo que se considera erróneamente como ataque[26].

- Falso Negativo: Ataque que no detecta el *IDS*[27].

- *Nmap*: Herramienta para el escaneo de puertos y servicios que permite el descubrimiento de red y ejecución de auditorías de seguridad. Con *Nmap* se puede determinar los hosts alcanzables en una red, servicios, sistemas operativos y *firewall* utilizados.[28].

- *Nessus*: Herramienta de *hacking* ético utilizada para el análisis de vulnerabilidades en la red encontrar fallos en configuraciones, *malware* ataques *DDoS* o fugas de información sensible.[29].

---

[24] ESCRIVÁ Op. cit., p.7.
[25] ESCRIVÁ Op. cit., p.7.
[26] ESCRIVÁ Op. cit., p.7.
[27] ESCRIVÁ Op. cit., p.7.
[28] ESCRIVÁ Op. cit., p.7.
[29] ESCRIVÁ Op. cit., p.7.

- *Wireshark*: Herramienta que permite el escaneo de tráfico de red para analizar los paquetes y sus componentes, los administradores de red la utilizan para realizar un análisis detallado de los paquetes y encontrar problemas en su transmisión [30].

- *Metasploit*: Herramienta utilizada para simular ataques en escenarios reales para encontrar vulnerabilidades y explotarlas[31].

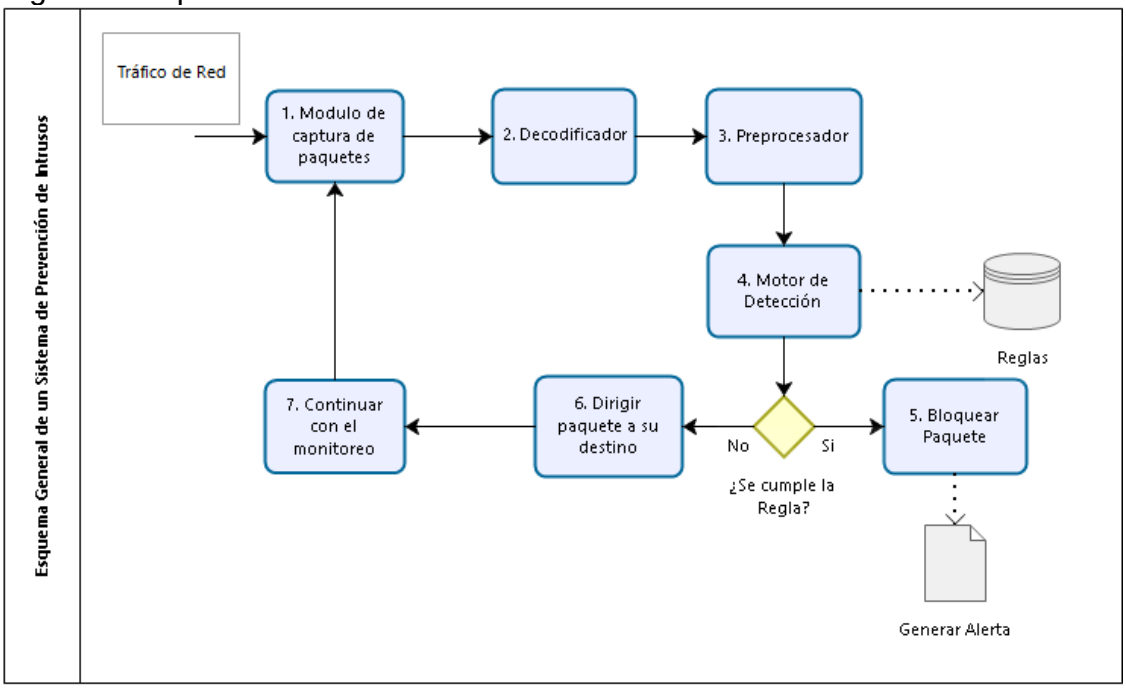
5.6 ESTADO DEL ARTE

Los sistemas de prevención de intrusos por sus siglas en ingles *Intrusion Prevention System (IPS)* fueron creados para fortalecer los esquemas de seguridad perimetral, con capacidad de detección y bloqueo de tráfico anómalo en la red, las alertas generadas son enviadas al correo electrónico del administrador, lo cual permite la activación de los planes de respuesta a incidentes de seguridad. Es decir, que estos sistemas monitorean el tráfico de la red generando respuestas frente a patrones de tráfico no conocido, facilitando a los administradores el monitoreo de la red en tiempo real. A diferencia de los *IDS* que solo detectan intrusiones, estos son capaces de bloquearlas en tiempo real, funcionan a nivel de la capa de aplicación, estos actúan como un Sniffer que analiza los protocolos, identificando paquetes infectados, algunos *IPS* permiten establecer reglas al igual que los *Firewalls*. Los IPS permiten fortalecer los esquemas de seguridad en conjunto con los Cortafuegos combinados forman una potente herramienta de detección de amenazas y vulnerabilidades.

[30] ESCRIVÁ Op. cit., p.7.
[31] ESCRIVÁ Op. cit., p.7.

La Figura 5 muestra el esquema general de un sistema de prevención de intrusos basado en red, el cual está compuesto por una fuente de datos que es el tráfico de red, un módulo que captura, un decodificador que identifica los protocolos y pasa los paquetes clasificados al módulo de detección, el cual utiliza reglas para detectar anomalías en los paquetes y tomar la acción de bloqueo.

Figura 5 Esquema General de un sistema de Prevención de Intrusos



Fuente: El Autor

5.5.1 *Snort*. Es un sistema de prevención y detección de intrusos de red que funciona en plataformas *Linux/Windows* bajo licencia *GPL*, utiliza el lenguaje de reglas para detección de ataques a nivel de capa de red o host, cuenta con el respaldo de una comunidad con el mayor número actualizaciones periódicas. *Snort* se ha convertido en el estándar de facto para la industria, tiene las siguientes

características: más de 700 firmas, ligero, distribución gratuita, análisis de tráfico en tiempo real, uso de filtros, y detección de *strings* o host arbitrarios[32].

Por otra parte, el proceso de detección de ataques inicia con la captura del tráfico en la capa de red a nivel de los protocolos: *ICMP, UDP y TCP/IP*. Luego, es procesado y analizado por cada uno de sus componentes. El motor de detección tiene la función de comparar el paquete capturado con una base de reglas y luego alertar de una posible intrusión para su bloqueo inmediato. El *Snor*t utiliza un fichero para su configuración, donde se especifican los parámetros de cada uno de los componentes necesarios para la correcta operación del sensor. A continuación, se describen cada uno de los módulos que integran este sistema, los cuales se encuentran contenidos en el archivo *snort.conf* de la siguiente manera:

- Módulo de Captura: se encarga de capturar los paquetes monitoreados en tiempo real.

- Decodificador de paquetes: recibe los paquetes del módulo *Libpcap* e identifica el tipo de protocolo: *ICMP, TCP, UDP* o *IP.*

- Preprocesador: almacena toda la información del paquete para su posterior procesamiento y análisis. Los datos de los paquetes que se tienen en cuenta por este componente son: protocolo, IP origen, IP destino, puerto origen y puerto destino.

- Motor de Detección: es el módulo principal del *Snor*t se encarga de analizar los paquetes enviados por el preprocesador y los compara con la base de firmas para tomar la acción de descartar o no el paquete.

[32] Snort IDS/IPS. (s.f.). Recuperado el 5 de Septiembre de 2016, de https://www.snort.org

- Sistemas de Alertas e Informes: se encarga de generar las alertas cuando se ha detectado un paquete sospechoso.

- Reglas: son los patrones o comportamientos que se deben buscar en los paquetes que son capturados y tiene la siguiente estructura:

  <Acción> <protocolo>
  <IP_Origen> <Puerto_Origen> - > <IP_Destino> <Puerto_Destino>
  {Opción_1; …; opción_N}

5.5.2 *Sourcefire Network Sensor*. Es un sensor de amenazas, uno de los más robustos del mercado, utiliza un método de detección basado en reglas, detecta tanto ataques conocidos como comportamientos anómalos. Las reglas permiten examinar los protocolos en las cabeceras de los paquetes y se pueden configurar para casos específicos de ataques o para estudiar las condiciones de un ataque. Comprende las siguientes características[33]:

- Instalación rápida.

- Interfaz basada en la Web.

- Técnica de análisis de datos e investigación informática.

- Creación de reglas, carga y gestión.

- Configuración de redes y alertas.

[33] Módulo de Seguridad Informática. (2008). Recuperado el 30 de Agosto de 2016, de http://www.cybsec.com/upload/ESPE_IDS_vs_IPS.pdf

- Redacción detallada de consultas e informes.

- Los sensores pueden desarrollarse como sistemas separados o en grupo de gestión centralizada de sensores remotos.

5.7. MARCO LEGAL

Para la implementación de este proyecto se tendrán en cuentan las leyes que protegen los datos y la integridad de los sistemas informáticos y de las sanciones a las personas que hagan uso de manera fraudulenta de los sistemas informáticos y las redes.

El proyecto se fundamenta en la Ley 1273 de 2009, la ejecución del proyecto estará acordes con las normas y requisitos legales de la actualidad. Por lo tanto, los registros que generará el sistema podrán ser requeridos como pruebas que ayudarán a localizar y sancionar a los responsables. Los siguientes son los artículos de Ley 1273 de 2009[34] que abarca el siguiente proyecto:

- Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMATICO
  Se comete cuando el intruso aprovecha la vulnerabilidad de los sistemas de información o falencias en los procedimientos de seguridad para el robo de información sensible o identidad.

- Artículo 269B: OBSTACULIZACION ILEGITIMA DE SISTEMA INFORMATICO O RED DE TELECOMUNICACION

[34] Ley 1273 de 2009. (2009). Recuperado el 29 de Agosto de 2016, de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Bloquear en forma ilegal o impedir el acceso a los sistemas informáticos y redes sin el debido consentimiento, ocasionando pérdidas e interrupciones de servicios a través de Internet.

- Artículo 269C: INTERCEPTACION DE DATOS INFORMATICOS
  Se cometen cuando se obstruyen datos sin autorización legal, durante la trasmisión de datos ente un remitente y receptor.

- Artículo 269E: USO DE SOFTWARE MALICIOSO
  Se refiera a la instalación o envío utilizando algún medio como el correo de virus, spyware, keylogger los cuales ocasionan daños o perdida de información sensible.

- Artículo 269G: SUPLANTACION DE SITIO WEB PARA CAPTURAR DATOS PERSONALES
  Crear un sitio web similar al de una entidad y enviar spam o correo engañoso, como ofertas de empleo y la victima suministra información, numero de cuentas y claves de seguridad para transferencias bancarias.

6. METODOLOGIA DE INVESTIGACION

Para el desarrollo de este proyecto de investigación se aplicó la metodología del tipo cuantitativa, dado que se puede medir en un determinado periodo el número de alertas presentadas en una red de datos, como también el tipo de ataque y los paquetes que fueron bloqueados por el sistema de prevención de intrusos.

Figura 6 Metodología de Investigación

Fuente: El Autor

La Figura 6 muestra cada uno de los pasos seguidos para obtener información relevante que luego se analizó con el fin de encontrar alternativas de solución al problema planteado. En primer lugar, se realizó una recopilación de toda la información del esquema de seguridad en red local de la empresa. Con el fin de identificar y analizar las capacidades de repuesta a eventos del sistema actual. También, se revisó la topología de la red, configuraciones y servicios activos. Luego, se determinó el tamaño de la población y muestra sobre la cual se debe aplicar el *IPS*, se utilizaron técnicas e instrumentos de recopilación de información que conducen a la solución de fortalecer la seguridad en la red de datos local de la empresa Minesa. A continuación, se describen cada uno de los pasos aplicados en la metodología:

1. Recopilación de Información: el proceso se realizó directamente en la sede de la empresa, se tuvo acceso a la documentación de las plataformas y arquitectura de la red, de donde se obtuvo la información de *Vlans*, topología de red, tecnología de virtualización, servidores y sistema de seguridad. Se investigó toda la parte teórica de un sistema de detección de intrusos para identificar el modo de operación y en qué punto de la red se puede ubicar para reforzar la seguridad en la red.

2. Definición de Población y Muestra: se identificó que la población está dada por la cantidad de servidores que pertenecen a esa *Vlan*, por encontrarse bajo el mismo dominio no fue necesario aplicar el estudio sobre una muestra.

3. Aplicación de técnicas e instrumentos de recolección de datos: como instrumento para recopilar información se utilizó la encuesta, el análisis se realizó por medio de la herramienta *Google Forms.* Otro de los métodos aplicado fue la observación directa de la documentación existente de las plataformas tecnológicas.

4. Resultados y análisis de encuesta: los resultados de la encuesta aplicada se pueden evidenciar en el Anexo E.

Por la naturaleza del proyecto que es aplicado, se investigaron las soluciones existentes de detección de intrusiones, se buscó la que más se adaptará al problema de monitoreo del tráfico en tiempo real en búsqueda de paquetes que contengan algún tipo de malware que pueda ser enviado desde los equipos que se encuentran dentro de la red y generar alerta en la consola, de esta manera se puede evidenciar el origen de la intrusión, puerto y protocolo al que es dirigido y así poder activar los planes de contingencia.

6.1 POBLACIÓN Y MUESTRA

La población está conformada por los once (11) servidores que proveen los recursos compartidos en la red de datos de la oficina de Bucaramanga, como se identificó que estos equipos se encuentran bajo un mismo dominio de red no es recomendable realizar el proyecto sobre una muestra, en cambio se estará realizando el análisis de tráfico que pasa a través de las interfaces del *IPS*.

6.2 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

La observación directa es una de las técnicas que se utilizó en este estudio para la recolección de datos, existe una documentación del esquema de seguridad de la empresa que contiene toda la información de la topología de red, canales de datos, arquitectura de servidores y equipos de comunicaciones, el enfoque se realizó sobre

la sede de Bucaramanga. Otras de las fuentes que se utilizaron la consulta de páginas web de seguridad. También, se realizó una encuesta a los miembros del área de TI para obtener información sobre el conocimiento y experiencia en seguridad informática, e identificar qué aspectos se pueden mejorar en el segmento de red donde encuentran los servidores de la compañía.

6.3 RESULTADO Y ANALISIS DE ENCUESTA

El día 15 de noviembre de 2016 se aplicó una encuesta a los integrantes del Departamento de TI de Minesa (Ver Anexo E) con el fin de conocer la opinión de cada miembro sobre el esquema de seguridad actual de la empresa y recabar información que ayude a buscar alternativas de soluciones de seguridad que ayuden a reforzar el nivel de protección de la red interna de la empresa. La herramienta que se utilizó para aplicar la encuesta fue *Google Forms*, en total fueron 7 preguntas enfocadas en conocer el nivel de seguridad de la red. La primera pregunta se debía responder dependiendo del criterio: Alto, Medio, Bajo y Otro. A partir de la segunda pregunta se debía responder de acuerdo con el nivel de conocimiento de seguridad informática que tiene cada miembro: Si, No, No responde u otro. Finalmente, se realizó un análisis y tabulación de los resultados.

6.4 TIPO DE INVESTIGACION

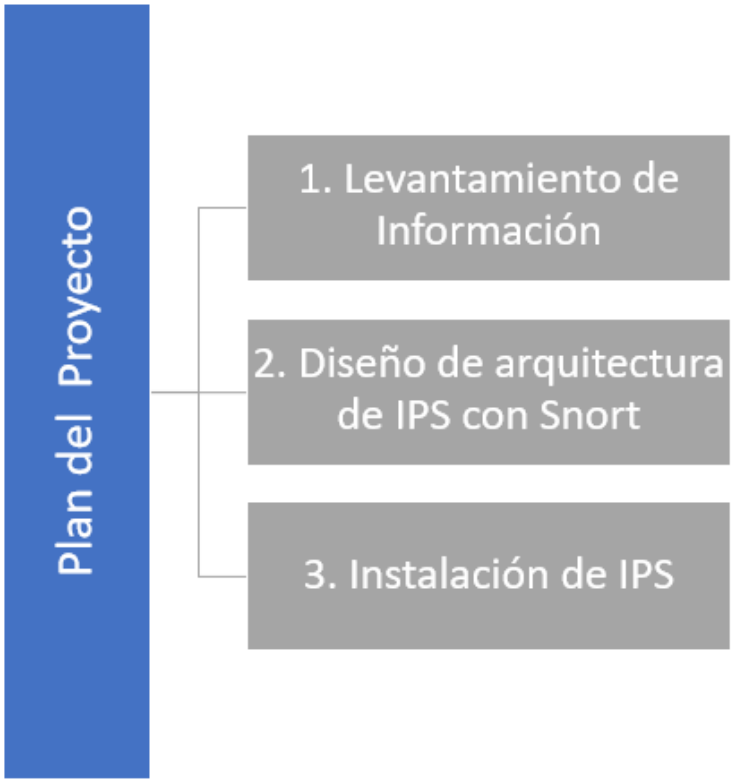
El tipo de investigación es descriptiva, se plantea un problema en donde el investigador se apoya en la recolección de datos sobre una población que está determinada por el número de servidores que están en *Vlan* de servidores en la Oficina de Minesa (Bucaramanga9, el método consiste en determinar la posibilidad

de instalar un sistema de prevención de intrusos *IPS,* para mejorar la seguridad en la red de la empresa Minesa S.A.S en Bucaramanga (Santander), se realiza un análisis de la población para identificar la opinión frente al fenómeno, para ello se estudiará el esquema de seguridad actual de la red. Los datos y la información de la investigación se obtuvieron directamente de la documentación del Departamento TI.

7. PLAN DE DESARROLLO DEL PROYECTO

El plan del proyecto está compuesto por tres (3) fases las cuales se pueden observar en la Figura 7, la primera inicia con una recopilación de información para conocer la infraestructura de la red, servicios que operan y esquema de seguridad actual, la segunda fase consiste en el diseño de una topología de red incluyendo un *IPS* que monitoree el tráfico de red que ingresa a la *Vlan* de servidores, la tercera y última es la instalación del *IPS* utilizando la arquitectura del *Snort v2.9* bajo el sistema operativo *Linux Ubuntu 16.04* en entorno virtualizado con *Vmware Esxi 6.0.*

Figura 7 Plan de desarrollo del proyecto

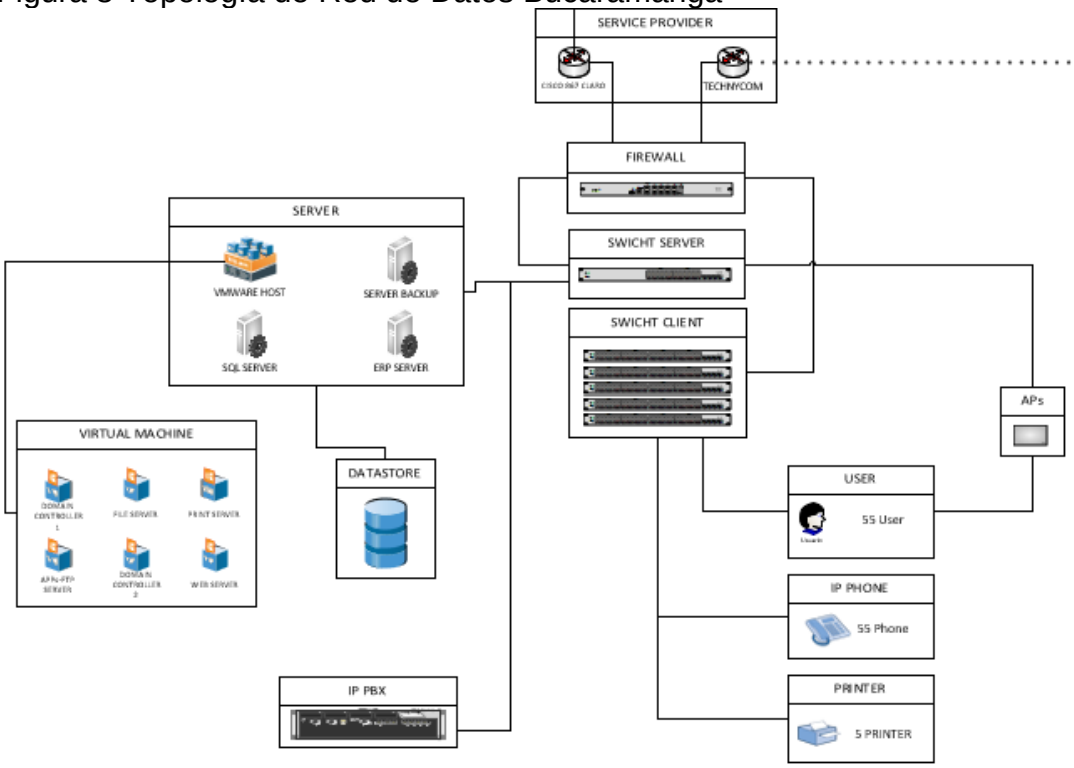


Fuente: El Autor

7.1 RECOPILAR INFORMACIÓN DEL ESQUEMA DE SEGURIDAD ACTUAL DE LA RED DE LA EMPRESA MINESA S.A.S

7.1.1 Esquema de Seguridad de La Red. La Figura 8 describe el sistema de seguridad de la Oficina de Bucaramanga, el cual está conformado por un firewall perimetral que conecta a la red corporativa con la red externa. Cuenta con dos (2) canales de Internet: principal y contingencia), existen dos (2) *Switches* para la conexión de los servidores y otro para la conexión de equipos clientes, *Ap´s* para el acceso a la red inalámbrica, servidores físicos y de virtualización y una unidad de almacenamiento *SAN*, planta telefónica que provee los servicios de telefonía, servicio de impresiones y acceso a la red corporativa a (55) usuarios.

Figura 8 Topología de Red de Datos Bucaramanga



Fuente: Departamento IT Minesa

7.1.2 Seguridad en los CPD. La empresa cuenta con Centro de Procesamiento de Datos (CPD) para cada una de las sedes, el acceso es controlado por control biométrico, sistemas de alarmas y contra incendios, con extintor para casos de emergencia, a estos se les lleva un control periódico para garantizar su efectividad ante cualquier eventualidad. Los servidores y equipos de comunicaciones se mantienen a temperaturas optimas con sistemas de aires acondicionados a los que se le realiza un mantenimiento preventivo cada tres (3) meses. Los equipos que se encuentran en el rack de servidores y comunicaciones cuentan con el respaldo de una *UPS* de *8KVA*, también se le realiza mantenimientos periódicos. El acceso a personal interno o terceros previamente debe ser autorizado y contar con el acompañamiento de personal de TI. Cualquier solicitud de cambio en algunos de los componentes de configuración, ya sea en servidores o en los equipos de comunicaciones debe ser previamente aprobado por el comité de cambios, el cual se reúne todos los martes y las aprobaciones se realizan los jueves.

En cuanto a sistemas de vigilancia, tiene cámaras y alarmas sensibles a movimientos que generan las alertas por email al personal de seguridad física para tomar las acciones y medidas preventivas. El control de acceso a los CPD utiliza lectoras de proximidad *HID* y contraseñas para garantizar la seguridad y protección de sus sistemas informáticos. La Tabla 1 contiene información de los puntos de red disponibles para conexión de cada uno de los servidores y clientes de cada una de las sedes.

Tabla 1 Puntos de Red de Datos de cada Sede de Minesa

BUCARAMANGA	HIGUERA	BOGOTÁ
85 puntos de red	70 puntos de red	40 puntos de red
8 servidores físicos	5 servidores físicos	1 servidor
60 usuarios	80	10

Fuente: Departamento TI Minesa

La empresa cuenta con dos (2) servidores físicos de virtualización y dos (2) para las copias de seguridad ubicados en las sedes Bucaramanga y California respectivamente como se muestra a continuación en la Tabla 2.

Tabla 2 Infraestructura Tecnológica de Servidores

SERVIDORES DE VIRTUALIZACIÓN			
DELL Power Edged R710 (Bucaramanga) Procesador Intel Xeon 8 CPU x 2.526 Ghz 50 GB RAM Hard Disk 6 TB Sistema Operativo: Vmware Esxi Vsphere 6.0	DELL Power Edged R710 (California) Procesador Intel Xeon 8 CPU x 2.526 Ghz 130 GB RAM Hard Disk 6 TB Sistema Operativo: Vmware Esxi Vsphere 6.0	Servidor de Backup (Bucaramanga) Procesador Intel Xeon 2 CPU x 2.53 GHz 16 GB RAM Hard Disk 300 GB Sistema Operativo: Microsoft Windows Server 2012 Estándar R2	Servidor de Backup (California) Procesador Intel Xeon 2 CPU x 2.53 GHz 16 GB RAM Hard Disk 300 GB Sistema Operativo: Microsoft Windows Server 2012 Estándar R2

Fuente: Departamento TI Minesa

7.1.3 Políticas de Red. El acceso a la red corporativa sólo está permitido a los equipos de cómputo propiedad de la compañía, los computadores se pueden conectar por red inalámbrica o cableada. Adicional, cuenta con una red invitado que brinda acceso al personal externo. Cada equipo tiene instalado el cliente antivirus,

firewall activado a nivel de sistema operativo y autenticación de usuarios para impedir que terceros puedan llegar a tener acceso a la red sin previa autorización. A nivel de red se tienen definidas las siguientes *VLAN*: Voz, Administración, Datos, *Wireless*, *Video -CFTV*, Servidores, *Backup*, *DMZ*, Impresoras, Invitados.

7.1.4 Servicios de Red

- *DHCP:* provee direccionamiento IP a los equipos de cómputo y telefonía de cada sede, el tiempo de expiración es de 8 días, con tolerancia a fallos.

- *VPN:* proporciona acceso a la red corporativa y recursos compartidos desde cualquier ubicación a través del protocolo *IPSec*, está disponible para los usuarios con computadores propiedad de la empresa previa autorización del gerente del área.

- *FILE SERVER:* brinda acceso a los archivos y carpetas compartidas de cada una de las áreas manteniendo la confidencialidad, disponibilidad e integridad de la información.

- *WEB:* La empresa cuenta con el sitio web http://minesa.com donde se publica la información corporativa y proyectos en los que se encuentra actualmente y a futuros.

- *FTP:* Este servidor permite el intercambio de información de la empresa con terceros, se encuentra en un entorno virtualizado.

- *SMTP:* se utiliza para el reenvío de documentos digitalizados por email y notificaciones de aplicaciones y sistemas que requieren ser monitoreados.

- *PRINT SERVER:* servidor para gestión centralizada de cola de impresión, facilita al usuario la impresión de documento por medio de código en blanco y negro y color, en los tamaños A4, A3, Carta y Oficio. En este servidor se encuentran instalado los plotters para impresión a gran escala que requieren las ares de Geología e Ingeniería.

- *TELEFONIA IP:* Servicios de llamadas locales, larga distancia, celulares e internacionales. El tráfico es enrutado con Calidad de servicio por los canales de datos hacia las diferentes plantas telefónicas ubicada en las distintas sedes.

- *VIDEOCONFERENCIA:* Servicios de llamadas por videoconferencia entre las diferentes sedes, el cual evita desplazamientos innecesarios e integran a todas las áreas de la compañía con las diferentes sedes.

7.2 DISEÑO DE RED PROPUESTO CON SISTEMA DE PREVENCION DE INTRUSOS IPS EN LA VLAN DE SERVIDORES

7.2.1 Descripción del sistema de Prevención de Intrusos. El sistema de prevención de intrusos que se instaló utiliza la arquitectura del *Snort v2.9* bajo sistema operativo *Linux Ubuntu 16.04* en un entorno de virtualización con *VMware Esxi 6.0*, realiza el monitorea el tráfico en tiempo real que ingresa a la Vlan de servidores, tiene dos (2) interfaces que sirven de puente entre las dos (2) redes, utiliza la librería de adquisición de datos *DAQ 2.0.6* para capturar el tráfico y las firmas de suscripción *snortrules-snapshot-29110* para usuario registrado.

7.2.2 Herramienta para el diseño del sistema de prevención de intruso. La herramienta que se eligió para la instalación del sistema de prevención de intrusos

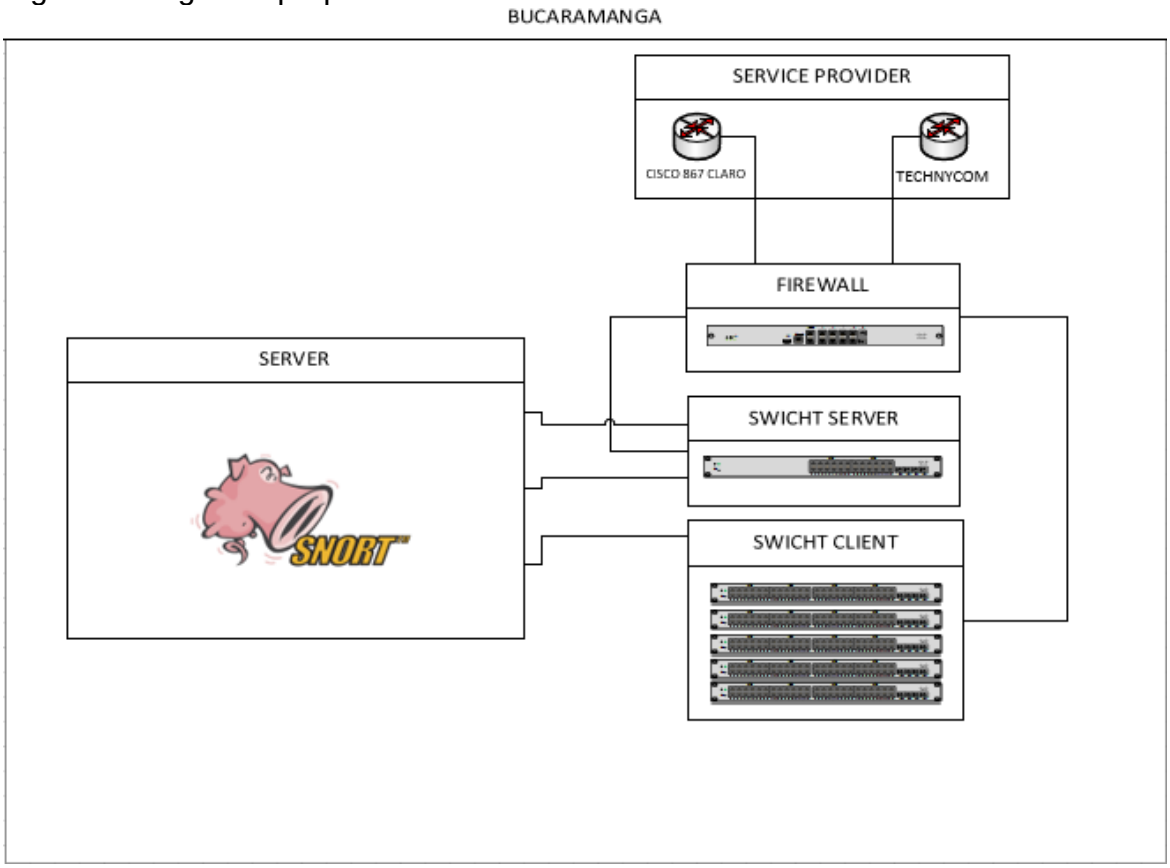
es el *Snort*, dado que es el estándar de facto en detección y prevención de intrusos con más de descargas a nivel mundial, es multiplataforma, con mayor soporte y por su efectividad en la detección de ataques, funciona bajo el sistema *Linux* y no requiere licencia para su operación, las reglas se descargan directamente desde el sitio oficial, utiliza un archivo de configuración para el monitoreo de la red. Se habilitó el modo de operación "*Inline",* el cual requiere dos (2) interfaces en modo promiscuo sin direccionamiento *IP* lo que impide que sea detectada.

7.2.3 Ubicación de Sistema de Prevención de Intrusos. se propuso un diseño de red con un Sistema de Prevención de Intrusos detrás del *Firewall*, para la supervisión del tráfico que pasa a la subred de servidores, la ubicación es la más recomendada dado que la empresa cuenta con sistema de prevención de intrusos que filtra las conexiones entrantes y salientes. El diseño propuesto refuerza la seguridad en la red local específicamente en la *Vlan* de servidores como medida de prevención frente a los posibles ataques que se originen desde el interior de la red, lo que mejora las capacidades de detección en la red local.

La Figura 9 describe la estructura general de la topología de red actual de la sede de Bucaramanga, que incluye un sistema de prevención de intrusos que asegura la Vlan de servidores de intrusiones, el tráfico que pasa es filtrado por el motor de detección, el cual se encarga de comparar los paquetes capturados con cada una de las firmas que detecta *malware* o código malicioso que pueda ser inyectado a los servidores por algún atacante o persona malintencionada. Vale destacar, Los componentes de la red, existen dos (2) *router* que proveen lo servicios de Internet principal y contingencia, un *Firewall* que asegura el perímetro, un *Switch* para el acceso a los servidores y cinco (5) *Switch* para los equipos clientes. Con este sistema el administrador de la red tiene mayor visibilidad de los eventos que pueden

estar presentándose en tiempo real en la red interna y ayuda prevenir problemas de seguridad y rendimiento de la red.

Figura 9 Diagrama propuesto con *Snort* ubicado detrás del F*irewall*.

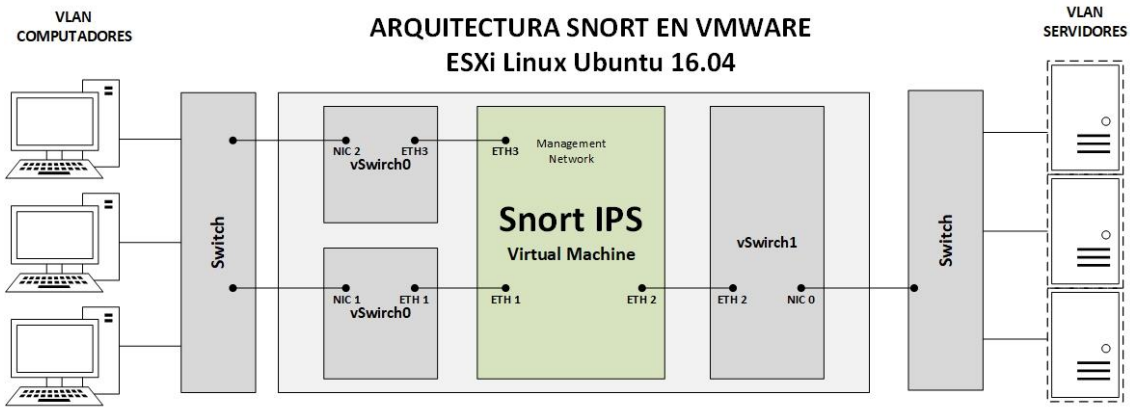


Fuente: Departamento de TI

El presente diseño plantea la instalación del *Snort* en *Host Vmware,* se utilizan dos (2) interfaces de red como un puente para monitorear el tráfico que ingresa a la *Vlan* de servidores. También, se incluye una tercera interfaz para la gestión de la máquina virtual, adicional se crean tres (3) *Virtual Switch* dos (2) de ellos en modo promiscuo, para pasar los paquetes entre Clientes y Servidores, el cual puede ser descartado por el motor de detección si se cumple alguna de las reglas. Para la captura de los paquetes en la capa de enlace se utilizó el módulo *DAQ,* en el archivo

de configuración se hablita el modo *Inline.* Con el diseño planteado se pueden controlar los paquetes y evitar accesos no autorizados.

Figura 10 Diseño de Arquitectura *Snort IPS* en *VMware Esxi 6.0*



Fuente: El Autor

7.3 INSTALACION DEL SISTEMA DE PREVENCION DE INTRUSOS SNORT

7.3.1 Requerimientos del Sistema. *El Snort* se instaló en un entorno virtualizado *VMware Vsphere ESXi 6.0* bajo el Sistema Operativo *Linux Ubuntu* 16.04 como *NIPS* con tres (3) interfaces de red: La primera para administración de la maquina *Snort IPS*, la segunda monitorea el tráfico de red que entra a la *Vlan* de servidores y la tercera protege esta red de ataques o acceso no autorizados. Las siguientes son las especificaciones técnicas que debe tener la máquina virtual:

- *Intel Xeon* 1 *socket virtual* 2 *core processor.*

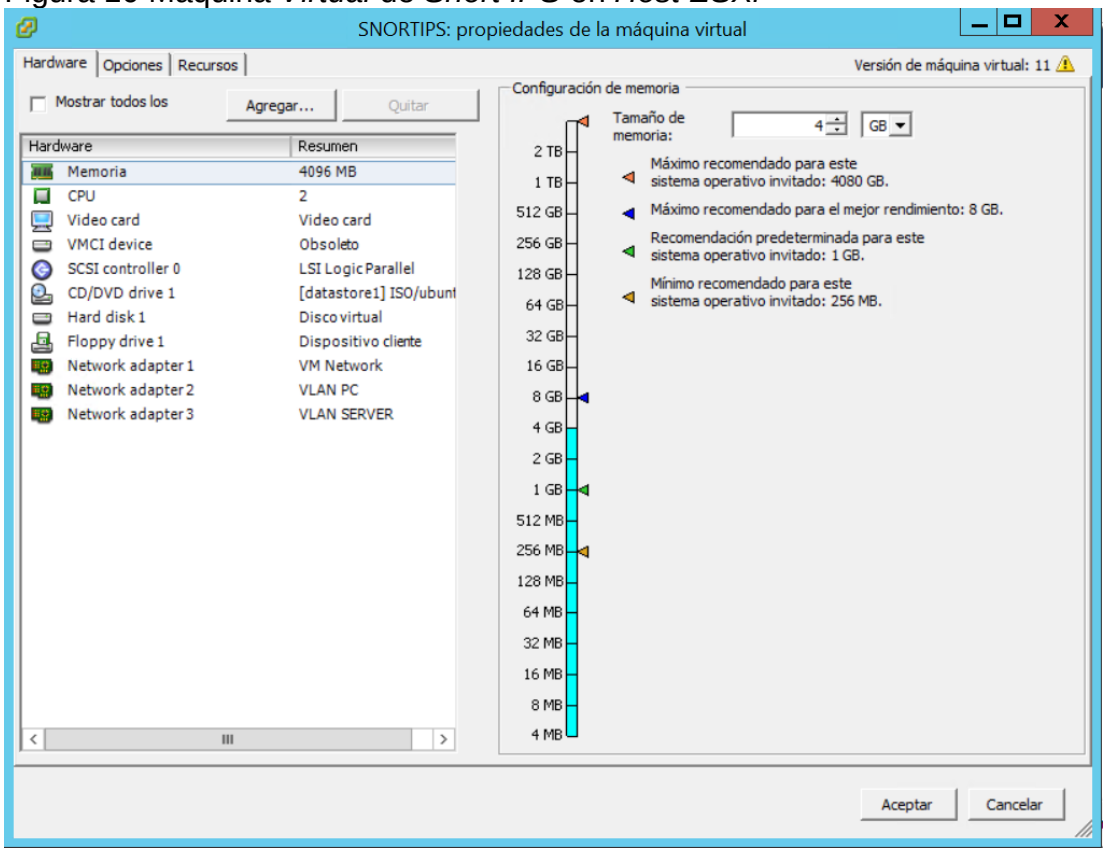
- 4 GB Memoria *RAM*

- 30 GB de Espacio en Disco Duro

- 3 tarjetas de red *Gigabit Ethernet*

7.3.2 Creación de Máquina virtual en Host Esxi. La Figura 10 muestra la maquina que se creó para la instalación del *Snort en modo IPS* con sus respectivas interfaces de red virtuales.

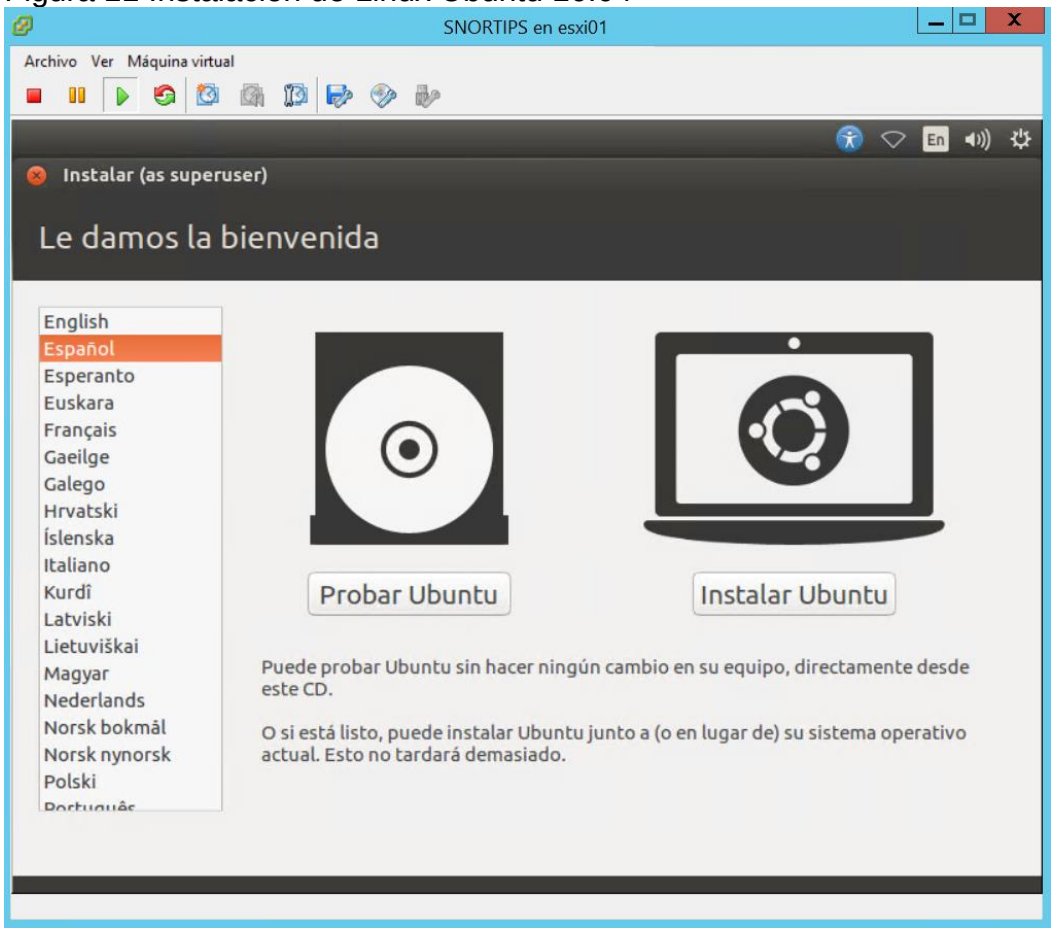
Figura 10 Máquina *Virtual* de *Snort IPS* en *Host ESXi*



Fuente: El Autor

7.3.3 Instalación de Ubuntu. La máquina virtual se arrancó desde la imagen *ISO* del Sistema Operativo *Linux Ubuntu 16.04*, el proceso de instalación se realiza en el idioma español en la versión de 64 *bits* como se muestra a continuación en La Figura 11.

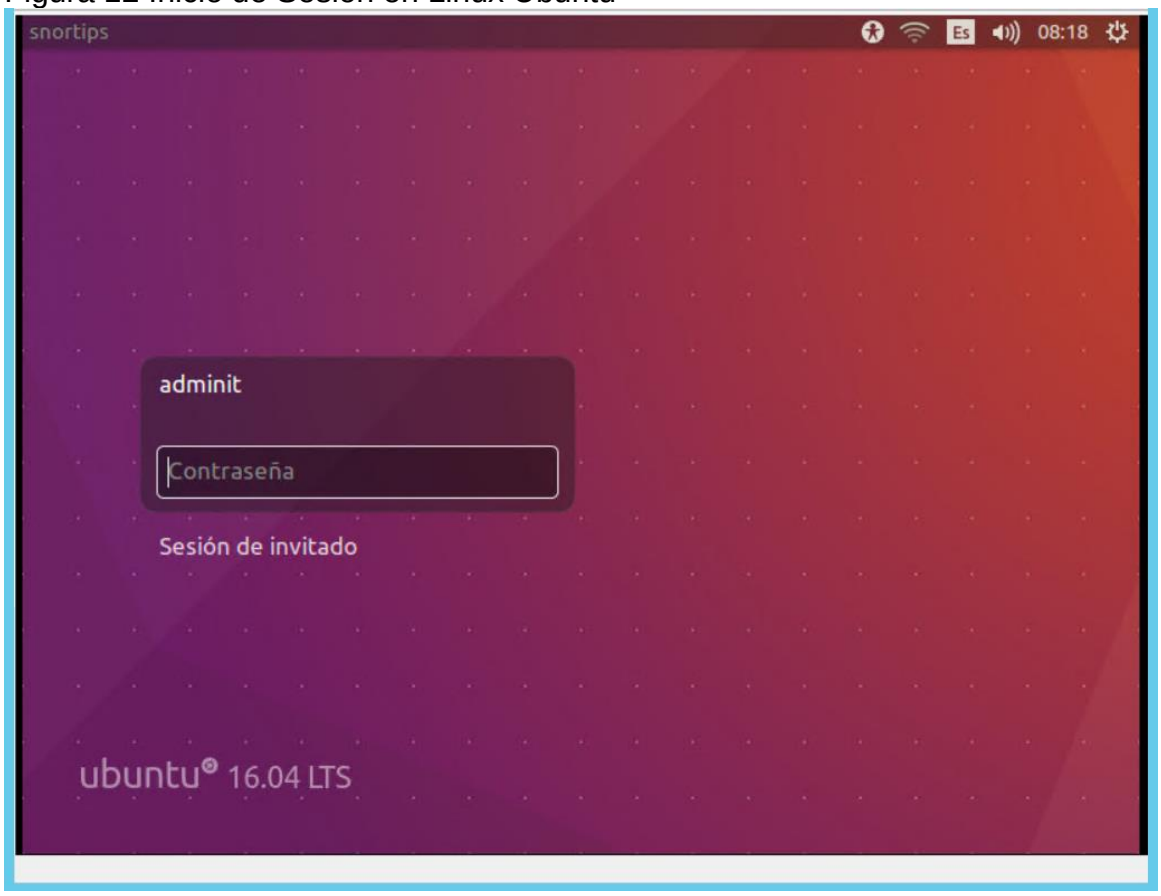
Figura 11 Instalación de Linux Ubuntu 16.04



Fuente: El Autor

Una vez culminada la instalación se inicia sesión con el usuario y contraseña definido en el sistema operativo Linux Ubuntu como se muestra a continuación en la Figura 12.

Figura 12 Inicio de Sesión en Linux Ubuntu



Fuente: El Autor

7.3.4 Configuración de Interfaces de Red. Para la configuración de las tarjetas de red se ejecutó el comando: *sudo vi /etc/network/interfaces.* La Tabla 3 describe cada uno de los comandos y parámetros utilizados. En primer lugar, se define la interfaz de gestión *ens160,* luego se habilita la Interfaz de monitoreo *ens192* en modo *gro off* y *lro off* para evitar el reensamble de paquetes antes de ser procesados y luego se reinicia el sistema con el comando *reboot*.

Tabla 3 Configuraciones de Interfaces de Red del *Snort IPS*

DESCRIPCION DE CONFIGURACIONES DE RED
Interfaz de gestión *auto ens160* *iface ens160 inet dhcp* # Interfaz modo puente Vlan de Clientes *auto ens192* *iface ens192 inet manual* *up ifconfig $IFACE 0.0.0.0 up* *up ip link set $IFACE promisc on* *post-up ethtool -K $IFACE gro off* *post-up ethtool -K $IFACE lro off* *down ip link set $IFACE promisc off* *down ifconfig $IFACE down* # Interface modo puente Vlan de Servidores *auto ens224* *iface ens224 inet manual* *up ifconfig $IFACE 0.0.0.0 up* *up ip link set $IFACE promisc on* *post-up ethtool -K $IFACE gro off* *post-up ethtool -K $IFACE lro off* *down ip link set $IFACE promisc off* *down ifconfig $IFACE down*

Fuente: http://sublimerobots.com/2016/02/snort-ips-inline-mode-on-ubuntu/

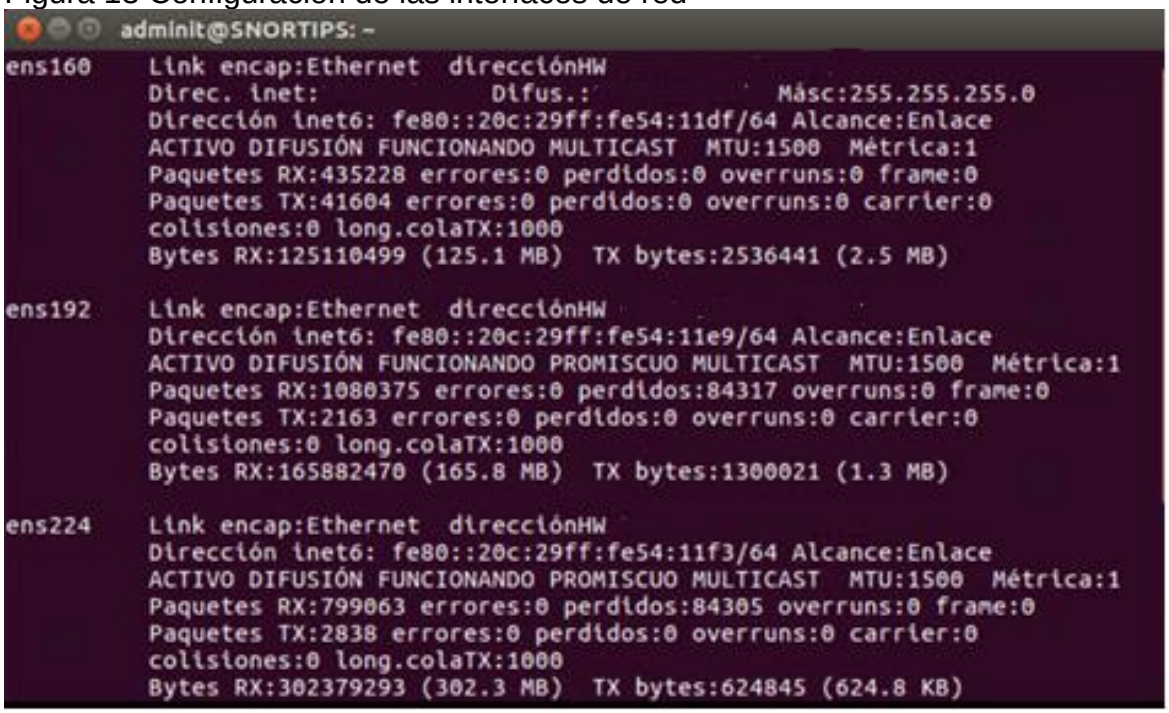
La Figura 13 muestra las configuraciones de cada interfaz de la siguiente manera:

- *ens160:* Interfaz de gestión el direccionamiento es por medio de dhcp.

- *ens192:* Interfaz en el segmento de red clientes utilizada como tráfico de ingreso.

- *ens224:* Interfaz de salida, el tráfico que pasa por esta tarjeta es controlado por el Snort a través del motor de detección.

Figura 13 Configuración de las interfaces de red



Fuente: El Autor

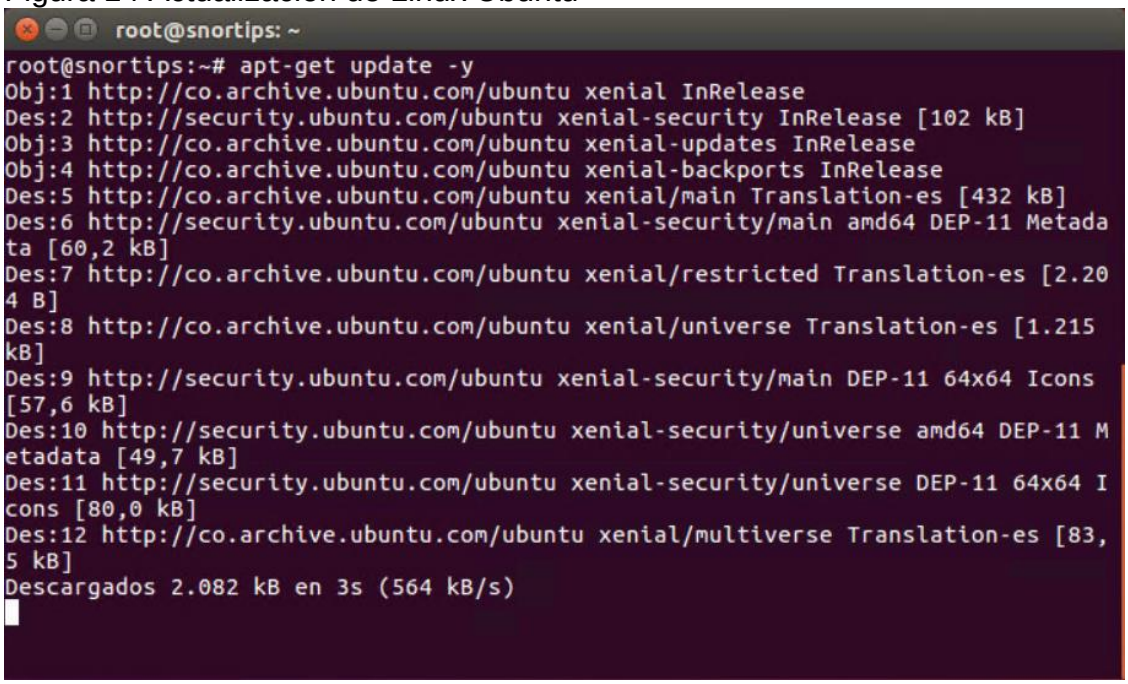
Las interfaces *ens192* y *ens224* no tienen dirección IP, ambas tienen habilitado el modo promiscuo. La interfaz ens160 se utiliza para la gestión de la máquina virtual.

Nota: por políticas de seguridad de la compañía esta información no puede ser revelada, la imagen fue editada para evitar divulgar información de direcciones *IP y MAC.*

7.3.5 Actualización de Ubuntu. La Figura 14 muestra el proceso de actualización de la Máquina virtual en *Ubuntu 16.04* requerido para una correcta instalación del *Snort*. Se utilizaron los siguientes comandos:

apt-get update -y
apt-get upgrade -y

Figura 14 Actualización de Linux Ubuntu



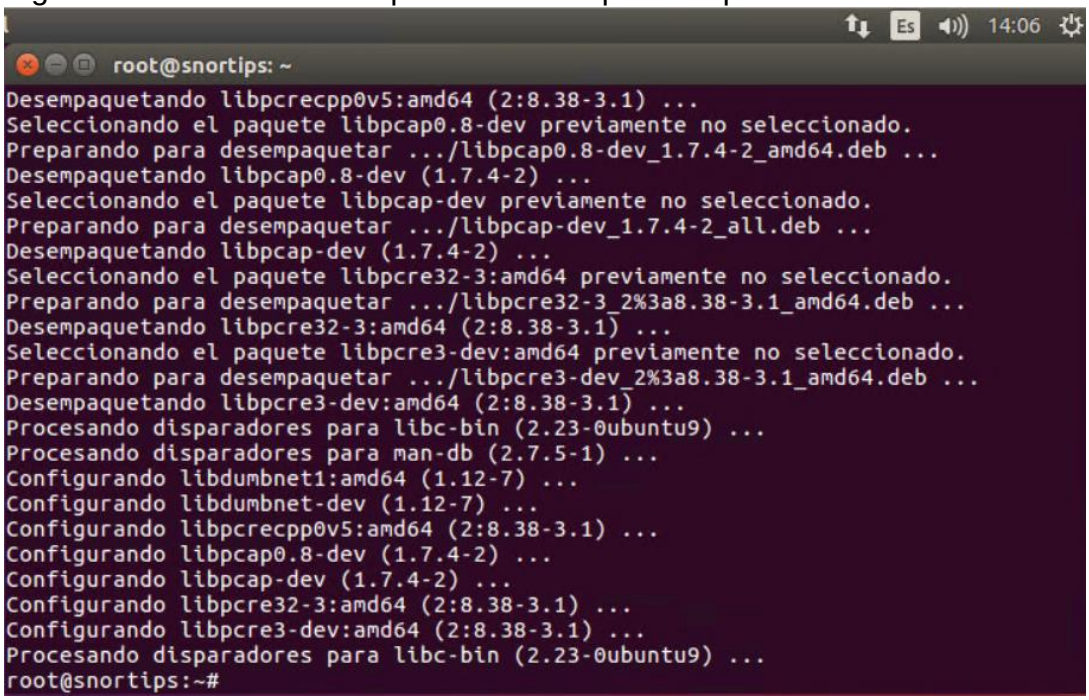
Fuente: El Autor

7.3.6 Instalación de las Dependencias del Snort. La Figura 15 muestra las librerías que aplica el *Snort* para capturar los paquetes en la capa de enlace, seguido se ejecuta el análisis con el motor de detección; este componente es el encargado de detectar si existe alguna anomalía en el paquete que debe ser bloqueada. A continuación, se muestran los comandos utilizados:

sudo apt-get install -y libpcap-dev libpcre3-dev libdumbnet-dev
sudo apt-get install -y bison flex

La Figura 15 muestra el progreso de la instalación de las librerías utilizadas por el Snort para capturar el tráfico en la capa de enlace.

Figura 15 Instalación de dependencias requeridas por el Snort



Fuente: El Autor

La Tabla 4 contiene una breve descripción de cada una de las dependencias que utiliza el *Snort* para capturar el tráfico y las funciones que cumplen, entre ellas la de pasar los paquetes al módulo decodificador, facilitando la tarea del preprocesador, que se encarga de pasar los paquetes al motor de detección para su respectivo análisis.

Tabla 4 Descripción de dependencias requeridas por Snort

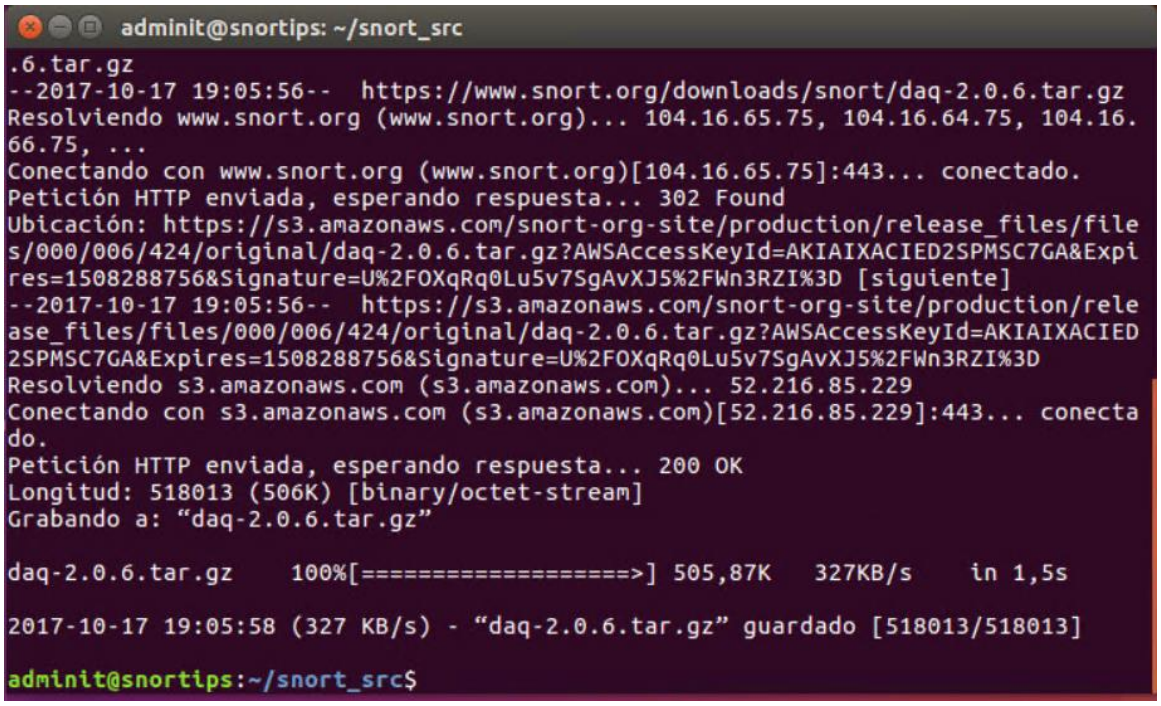
PREREQUISITO	DESCRIPCION
BUILD-ESSENTIAL :	proporciona las herramientas de compilación (GCC y similares) para compilar software.
BISON, FLEX :	Analizadores requeridos por *DAQ*
LIBPCAP-DEV	Biblioteca para la captura de tráfico de red requerida por Snort.
LIBPCRE3-DEV :	Biblioteca de funciones para soportar las expresiones regulares requeridas por Snort.
LIBDUMBNET-DEV :	La biblioteca *libdnet* proporciona una interfaz simplificada y portátil para varias rutinas de red de bajo nivel. Muchas guías para instalar Snort instalan esta biblioteca desde el origen, aunque eso no es necesario.
ZLIB1G-DEV :	Una biblioteca de compresión requerida por Snort.
LIBLZMA-DEV :	Proporciona descompresión de archivos *swf (adobe flash)*
OPENSSL Y LIBSSL-DEV :	Proporciona firmas de archivos SHA y MD5

Fuente: https://www.snort.org/documents/snort-2-9-9-x-on-ubuntu-14-16

El DAQ (Data AcQuisition library): es la librería requerida por el *Snort* para capturar el tráfico que luego será analizado por el sensor, para validar si existe algún paquete malicioso que necesite ser descartado, la descarga se realizó con el siguiente comando:

wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz

Figura 16 Descarga de librería del *Snort*



Fuente: El Autor

Después de la descarga de *DAQ* el siguiente paso es descomprimir el paquete y compilarlo como se muestra a continuación:

tar -xvzf daq-2.0.6.tar.gzv
./configure
make
Sudo make install

Finalmente, se instalan los prerrequisitos adicionales que mejoran el rendimiento del Snort con el siguiente comando:

Sudo apt-get install -y zlib1g-dev liblzma-dev openssl libssl-dev

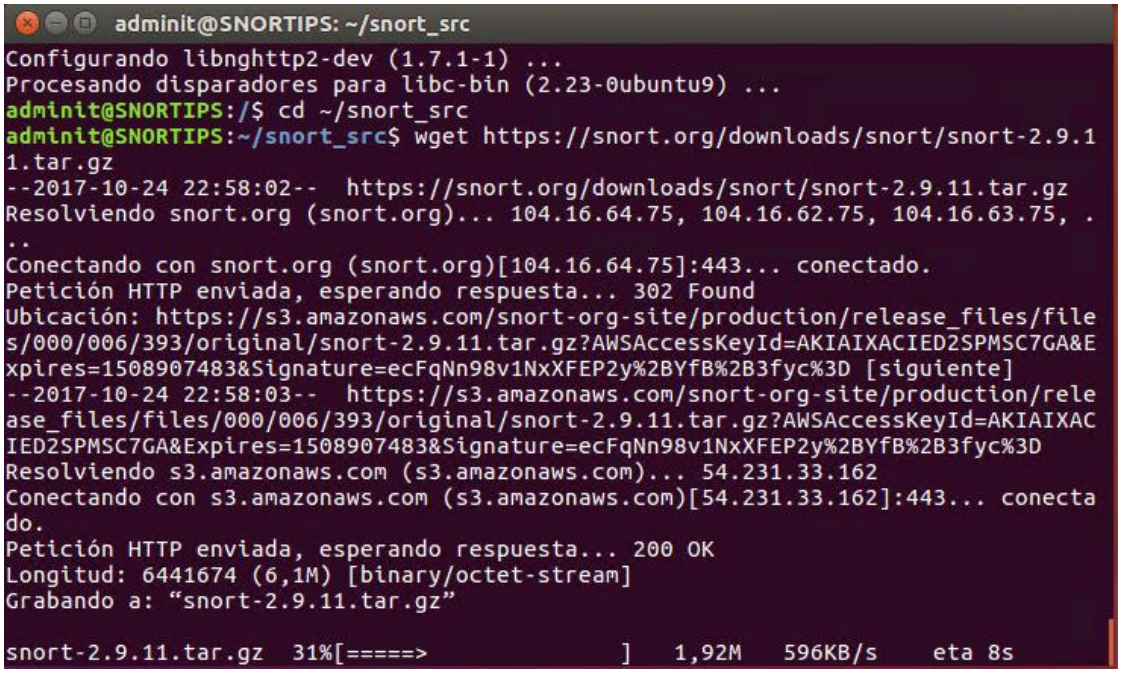
7.3.7 Instalación de Snort. Antes de instalar el *Snort* se creó el directorio *snort_src*, el cual se utilizó para descargar los paquetes del *Snort*, La Figura 17 muestra la ejecución de los comandos[35]:

mkdir ~/snort_src

cd ~/snort_src

wget https://www.snort.org/downloads/snort/snort-2.9.11.tar.gz

Figura 17 Creación de directorio “snort_src” y descarga de Snort



Fuente: El autor

Finalizada la descarga del instalador se descomprimió el paquete y luego se compiló con los siguientes comandos:

[35] Instalación Snort 2.9 en Ubuntu 16.04. (7 de Enero de 2017). Recuperado el 2 de Abril de 2017, de https://www.snort.org/documents/snort-3-on-ubuntu-14-and-16

tar -xvzf snort-2.9.11.tar.gz

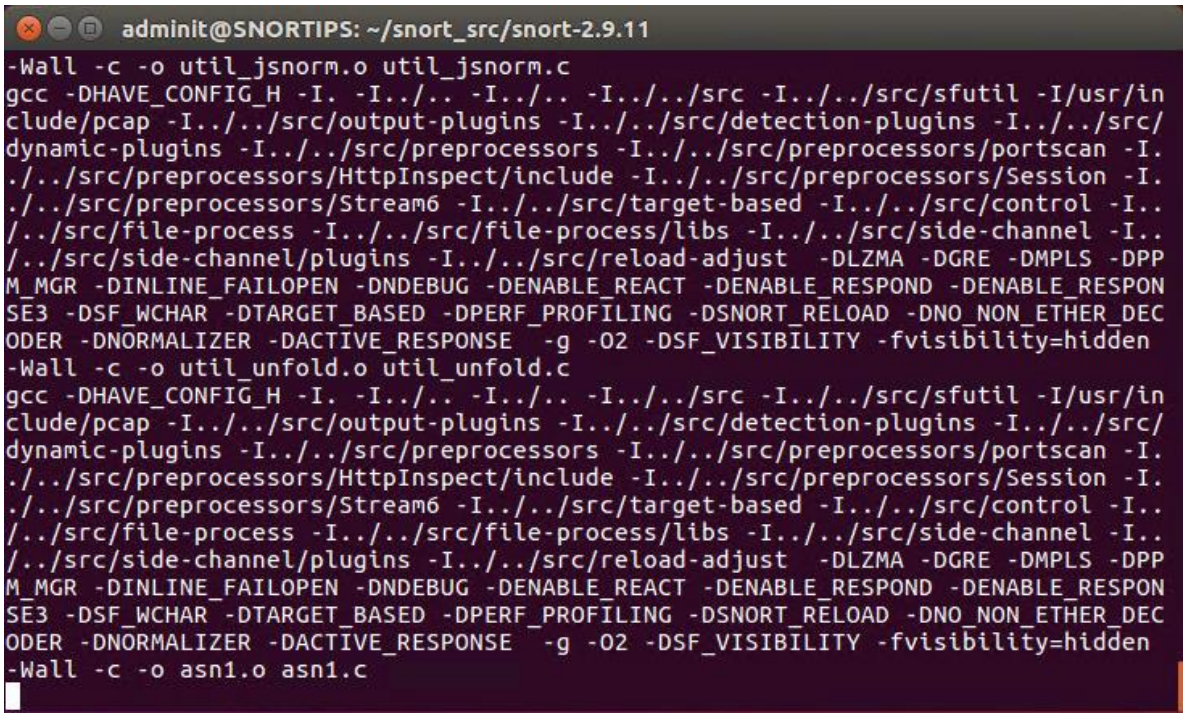
cd snort-2.9.11

./configure --enable-sourcefire

make

sudo make install

Figura 18 Complication del Snort



Fuente: El Autor

La Tabla 5 muestra los comandos para creación de cada uno de los directorios que requiere el Snort para su correcto funcionamiento, el cual incluye donde se almacenan las reglas, preprocesadores, logs y listas de UPS entre otros.

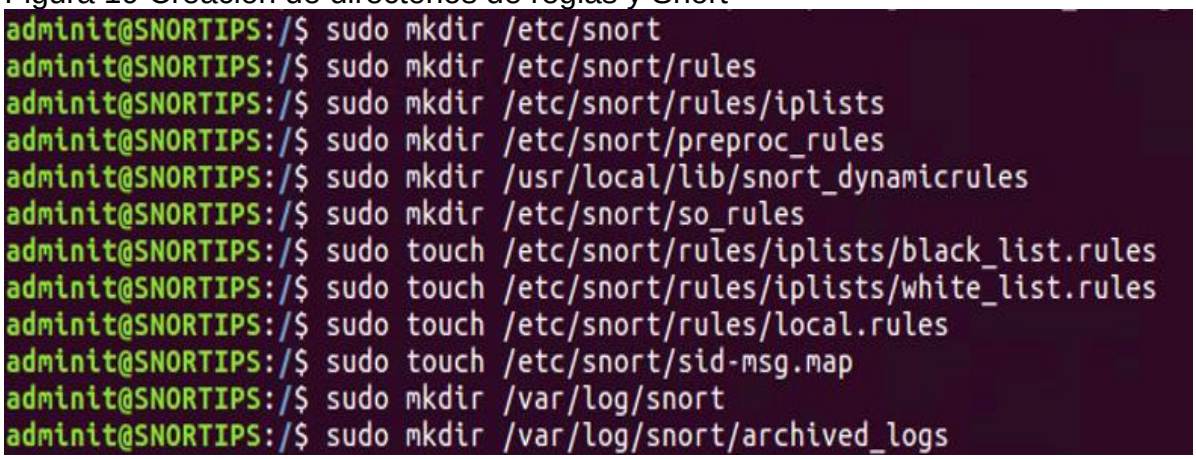
Tabla 5 Creación de directorios para archivo de configuración y reglas

DESCRIPCION	COMANDOS
Creación de directorios del *Snort*	*Sudo mudar /etc/Snort*
	Sudo mkdir /etc/Snort/rules
	Sudo mkdir /etc/Snort/rules/iplists
	Sudo mkdir /etc/Snort/preproc_rules
	Sudo mkdir /usr/local/lib/Snort_dynamicrules
	Sudo mkdir /etc/Snort/sid-msg.map
Creación del archivo para almacenar reglas y Listas de *IP*	*sudo touch /etc/snort/rules/iplists/black_list.rules*
	sudo touch /etc/snort/rules/iplists/white_list.rules
	sudo touch /etc/snort/rules/local.rules
	sudo touch /etc/snort/sid-msg.map
Creación de directorio de salida de logs	*sudo mkdir /var/log/snort*
	sudo mkdir /var/log/snort/archived_logs

Fuente: https://www.snort.org/documents/snort-2-9-9-x-on-ubuntu-14-16

La Figura 19 muestra la creación exitosa de los directorios que requiere el Snort para almacenar los archivos de reglas, preprocesadores y configuración entre otros.

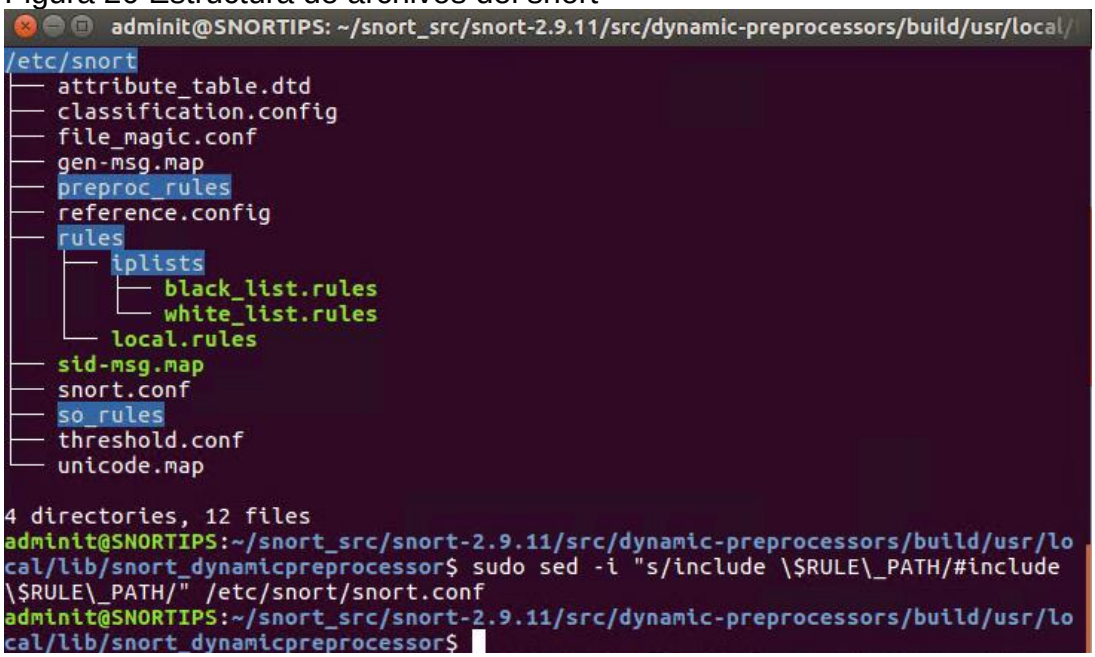
Figura 19 Creación de directorios de reglas y Snort



Fuente: El Autor

Después de creado los directorios del *Snort* se comprueba que la estructura de se encuentre correctamente con el comando *tree* como se observa a continuación en La Figura 20.

Figura 20 Estructura de archivos del snort



Fuente: EL Autor

7.3.8 Configuración del *Snort.conf.* En este archivo se configuró los módulos requeridos para analizar el tráfico, se habilitó el modo *Inline*, para que trabaje como *NIPS* (Sistema de Prevención de Intrusos en Red). La Tabla 6 describe cada una de las configuraciones que se realizaron en el archivo *snort.conf*. En primer lugar, se define la variable de la red a monitorear con su respectiva mascara de red, luego se añaden las rutas de los directorios de las reglas preprocesadores y listas de *IPs*,

seguido se deben descomentar las líneas de los preprocesadores de los protocolos *TCP/IP versión 4 y 6*[36]*.*

Tabla 6 Parámetro de configuración de *"snort.conf"*

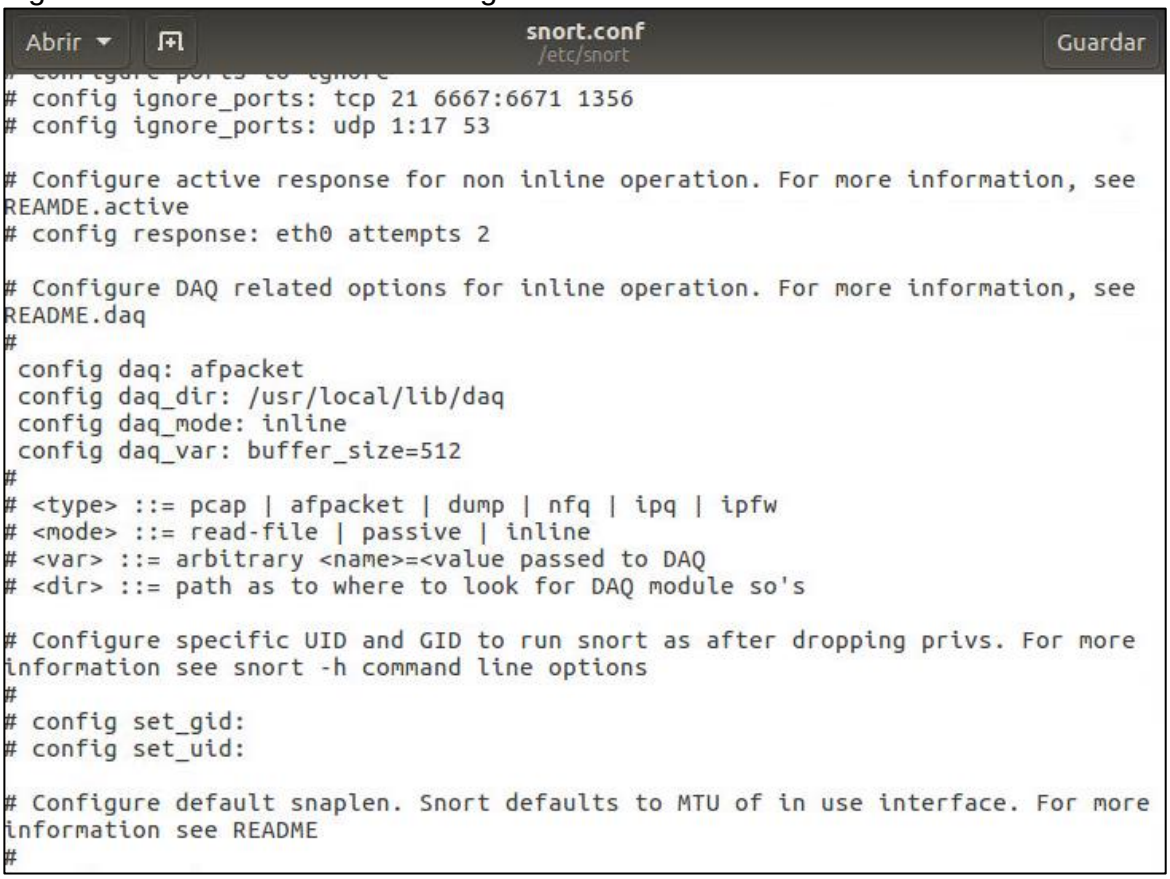
	DESCRIPCION	PARAMETROS
1.	Variables de red	*ipvar HOME_NET xx.xx.xx.xx* *ipvar EXTERNAL_NET !$ HOME_NET*
2.	Rutas de archivos del *Snort*	*var RULE_PATH /etc/snort/rules* *var SO_RULE_PATH /etc/snort/rules /so_rules* *var PREPROC_RULE_PATH /etc/snort/rules* *preproc_rules*
3.	Definición de ruta de listas blancas y negras	*var WHITE_LIST_PATH /etc/snort /rules/iplists* *var BLACK_LIST_PATH /etc/snort /rules/iplists*
4.	Preprocesadores	*preprocessor normalize_ip4* *preprocessor normalize_tcp: ips ecn stream* *preprocessor normalize_icmp4* *preprocessor normalize_ip6* *preprocessor normalize_icmp6*
5.	Configuración de modo *IPS (INLINE)*	*config daq: afpacket* *config daq_dir: /usr/local/lib/daq* *config daq_mode: inline* *config policy_mode: inline* *config daq_var: buffer_size=512*

Fuente: https://www.snort.org/documents/snort-2-9-9-x-on-ubuntu-14-16

La Figura 21 muestra las líneas que se deben descomentar y añadir en el archivo *snort.conf*, para definir modo *Inline,* los parámetros se definen en la sesión del *DAQ.*

[36] Snort IPS daq afpacket. (12 de Agosto de 2010). Recuperado el 2 de Abril de 2017, de https://www.snort.org/documents/snort-ips-using-daq-afpacket

Figura 21 Archivo creado de configuración de *Snort*

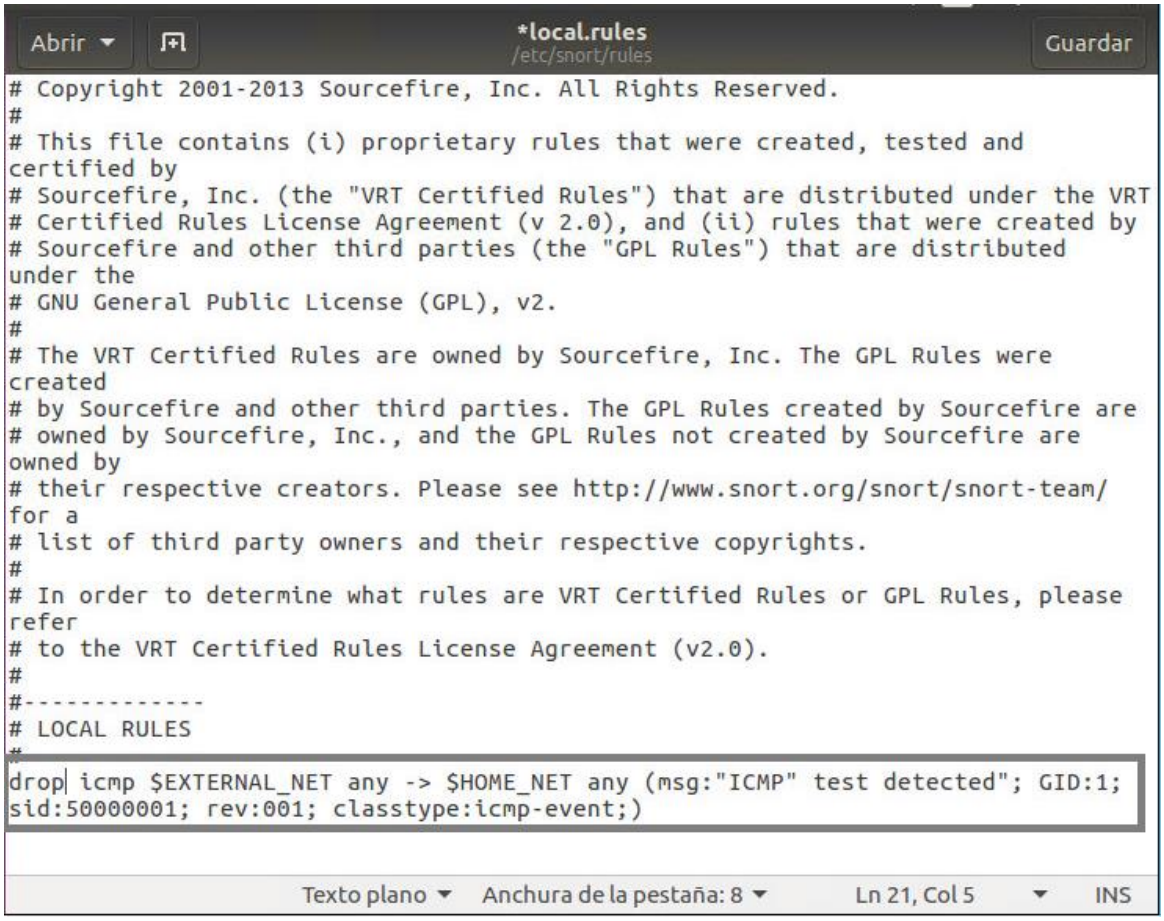


Fuente: El Autor

7.3.10 Creación de regla local. Para probar el funcionamiento como *IPS se* creó una regla local, la acción que debe tomar es la de bloquear los paquetes *icmp* que procedan de la dirección *IP* externa y hacia cualquier puerto de la red protegida. A continuación, se muestra la regla creada para realizar el *test*:

drop icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP test detected"; GID:1; sid:50000001; rev:001; classtype:icmp-event;)

Figura 22 Archivo de regla local "*/etc/snort/rules/local.rules"*



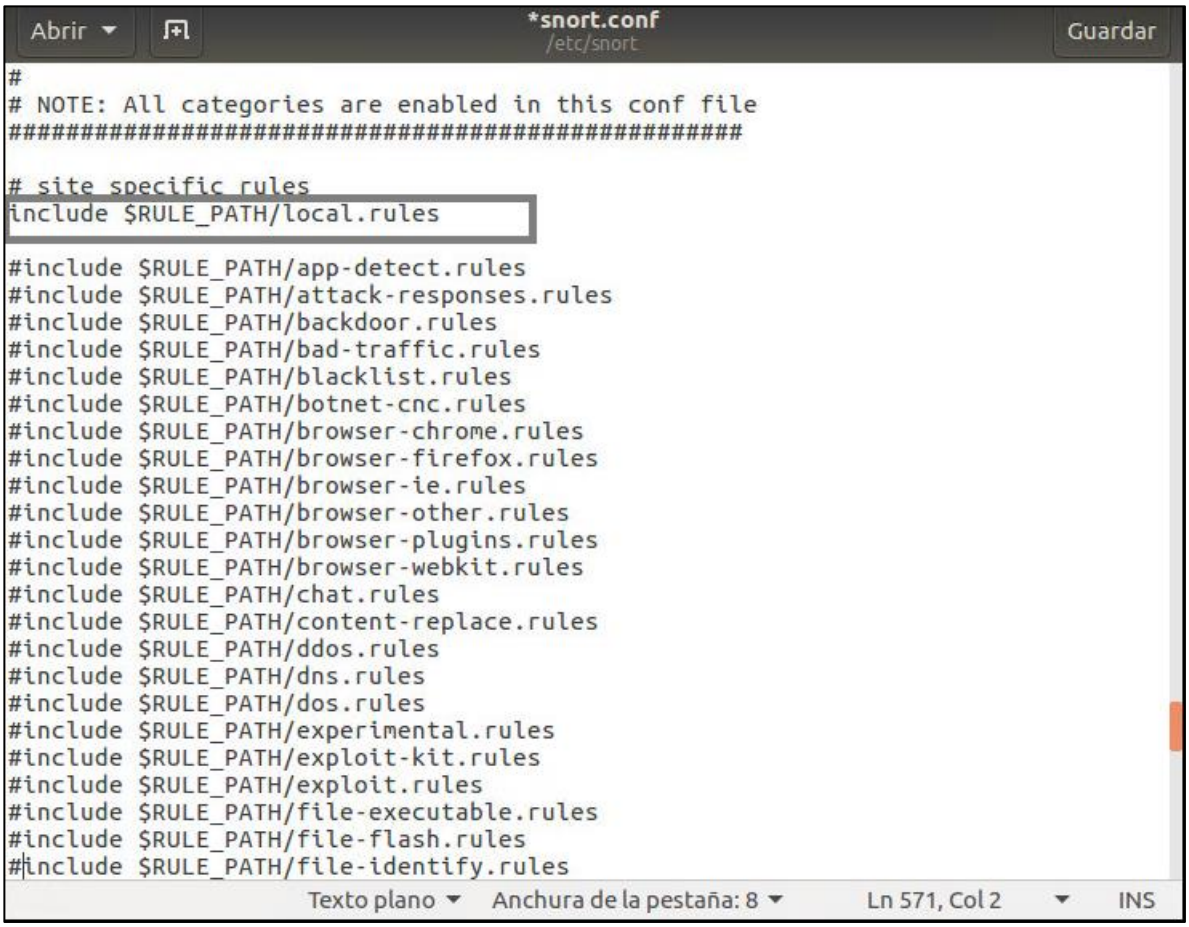
Fuente: El Autor

La Figura 22 muestra la estructura de una regla en snort, en primer lugar, se coloca la palabra reservada *drop* la acción es el bloquear todos los paquetes con cabecera *icmp,* seguido se coloca la dirección *IP* origen en este caso corresponde al tráfico que ingresa a la *Vlan* de servidores y el puerto origen. El símbolo "->" indica la

dirección de los paquetes. Después, se colocó la red destino, el mensaje que debe aparecer en la consola y los identificadores de la regla.

Se debe descomentar la regla local creada para que el Snort la reconoza como se muestra a continuación en la Figura 23.

Figura 23 Habilitación de regla local en archivo de *Snort*

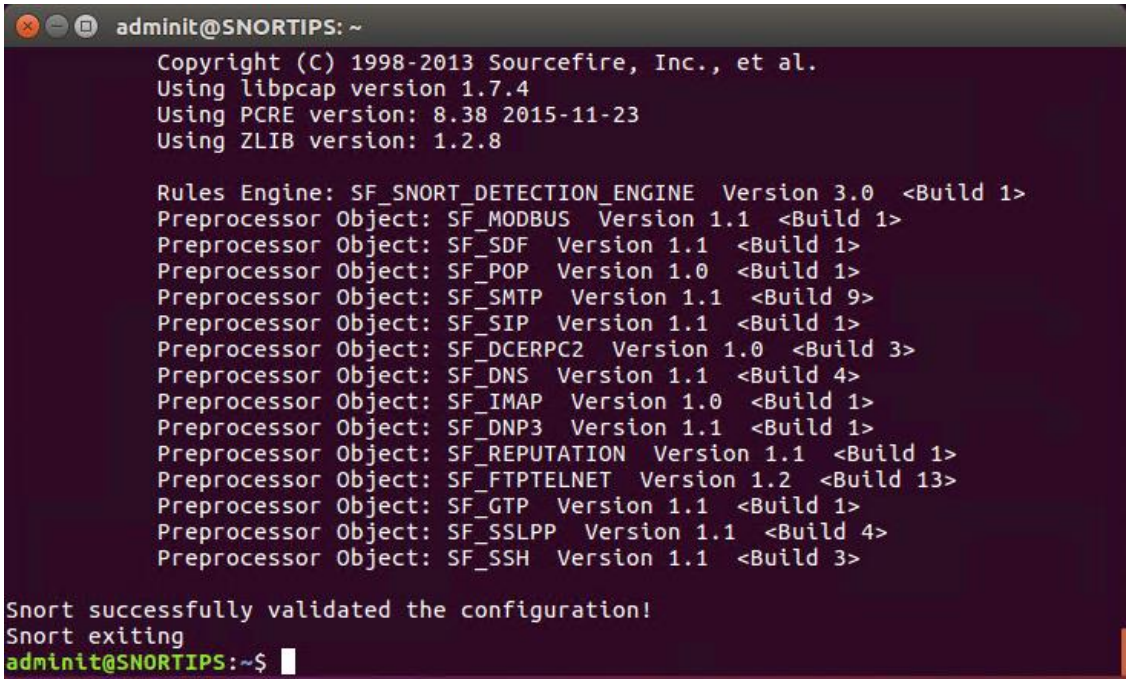


Fuente: El Autor

Después de terminar la configuración de los parámetros del *Snort* se debe validar que el archivo este configurado correctamente con el comando “*sudo snort -T -c*

/etc/snort/snort.conf -I ens192:ens224 -Q", como se muestra en La Figura 24. De esta manera, se garantiza que el Sistema hará cualquier tipo de detección de la regla activada en el archivo.

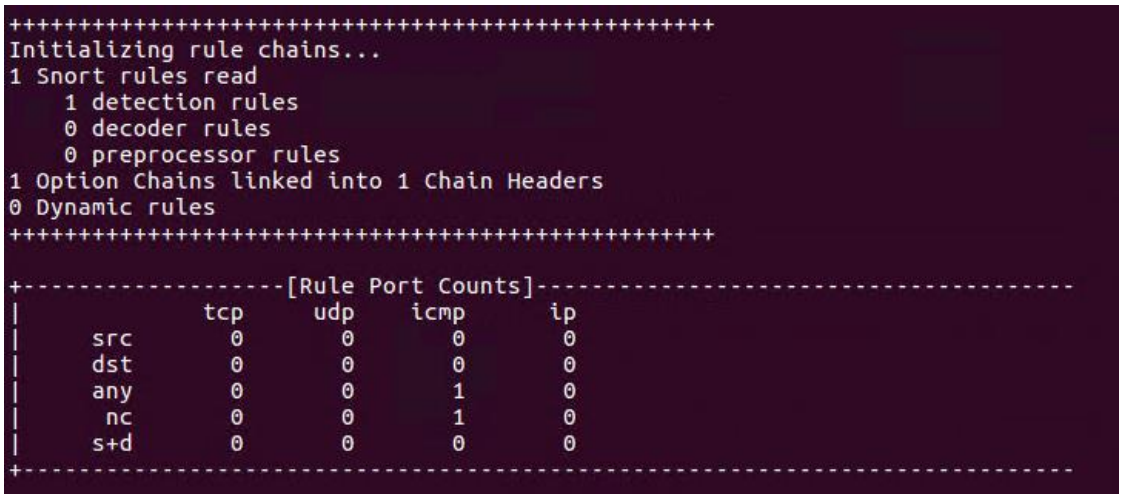
Figura 24 Resultado *Test* de validación de configuración del *Snort*



Fuente: El Autor

La Figura 25 muestra que la regla local creada anteriormente fue reconocida por el *Snort* sin ningún error, en la columna se observa que el bloqueo se aplica sobre el protocolo icmp sobre cualquier puerto. La validación se realizó con el siguiente comando:

Figura 25 Validación de Reglas Activas



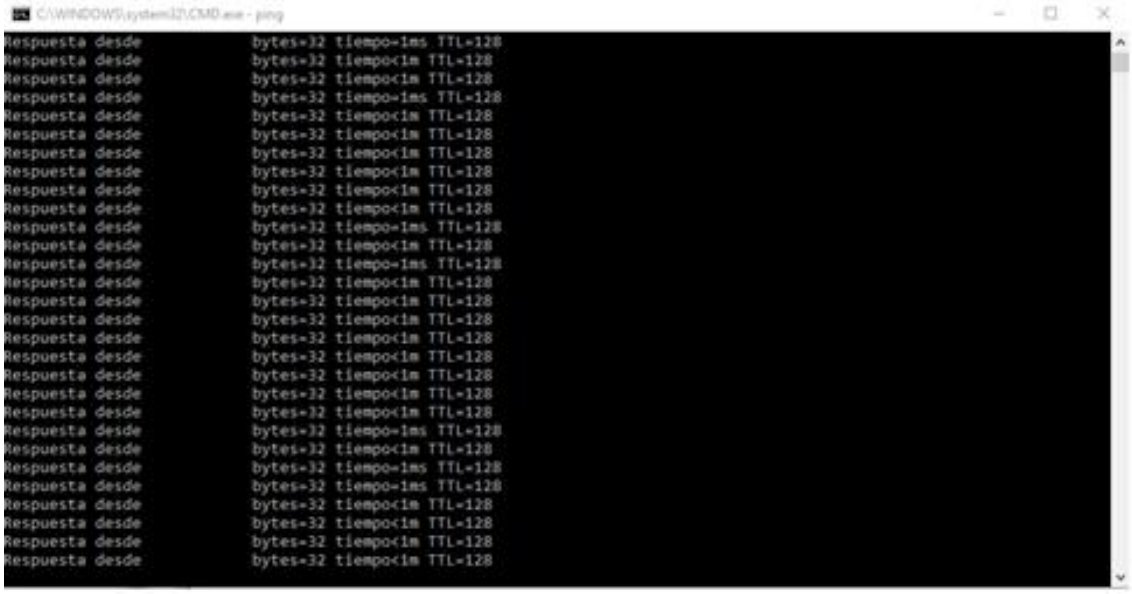
Fuente: El Autor

Con la regla configurada se puede validar que el modo *IPS* de *Snort* está activo, la regla bloquea cualquier paquete con protocolo *icmp* desde cualquier puerto y dirección *IP* externa que se dirija a la red protegida.

7.3.11 Prueba de IPS. La Figura 26 ilustra un ping realizado a uno de los servidores que se encuentra en la *Vlan* monitoreada con respuesta exitosa. Es decir, que no existe restricciones de respuesta de paquetes *icmp*.

Nota: Por políticas de seguridad las direcciones *IP* no pueden ser reveladas.

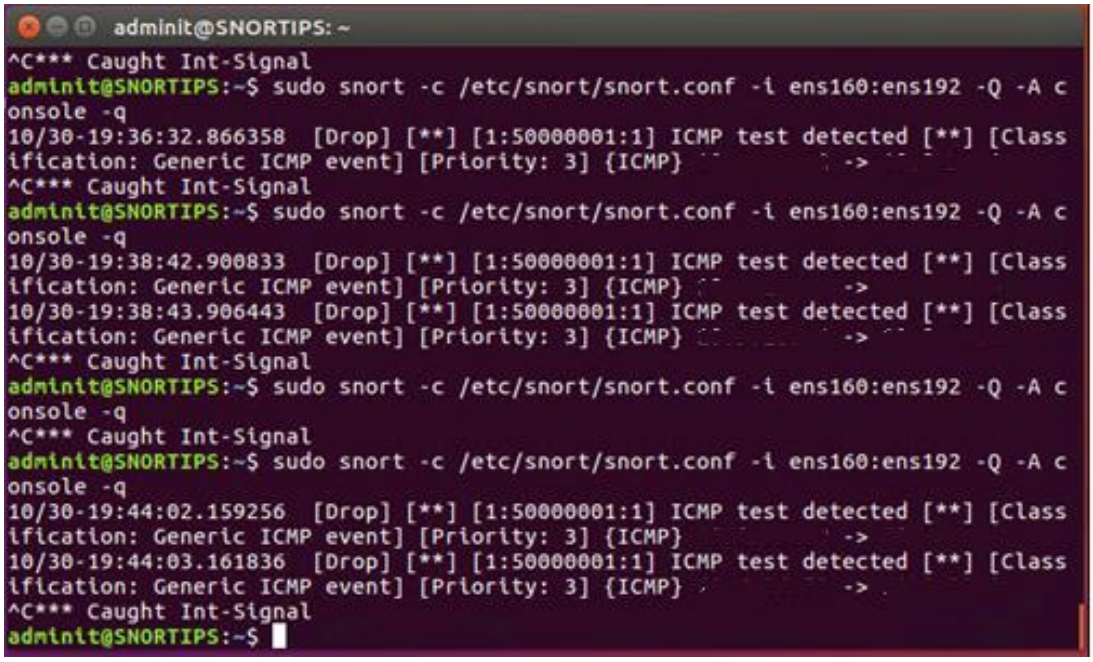
Figura 26 Resultado de un *Ping* a un *hos*t en la *Vlan* de Servidores



Fuente: El Autor

La Figura 26 muestra en la consola del *Snort* el momento en que el *IPS* detecta tres (3) paquetes que provienen de la *IP* origen al destino en la *Vlan* de Servidores, esto ocurre al momento de habilitar el Snort. La consola muestra la detección de actividad sospechosa sobre el protocolo *icmp* y realiza el bloqueo inmediato.

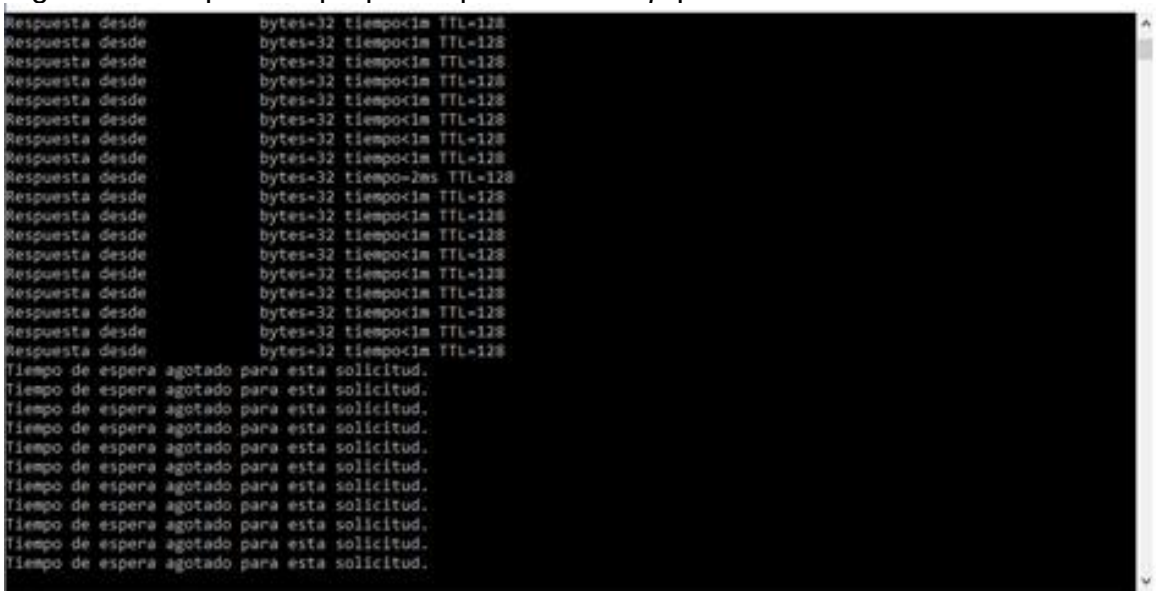
Figura 27 Consola del Snort haciendo bloqueo de un ping al host



Fuente: El Autor

Una vez habilitado el *Snort IPS* se observa en la gráfica que los paquetes son bloqueados con la acción *drop* sobre el protocolo *icmp*. La Figura 28 muestra la perdida de paquetes durante el monitoreo del tráfico por *Snort.*

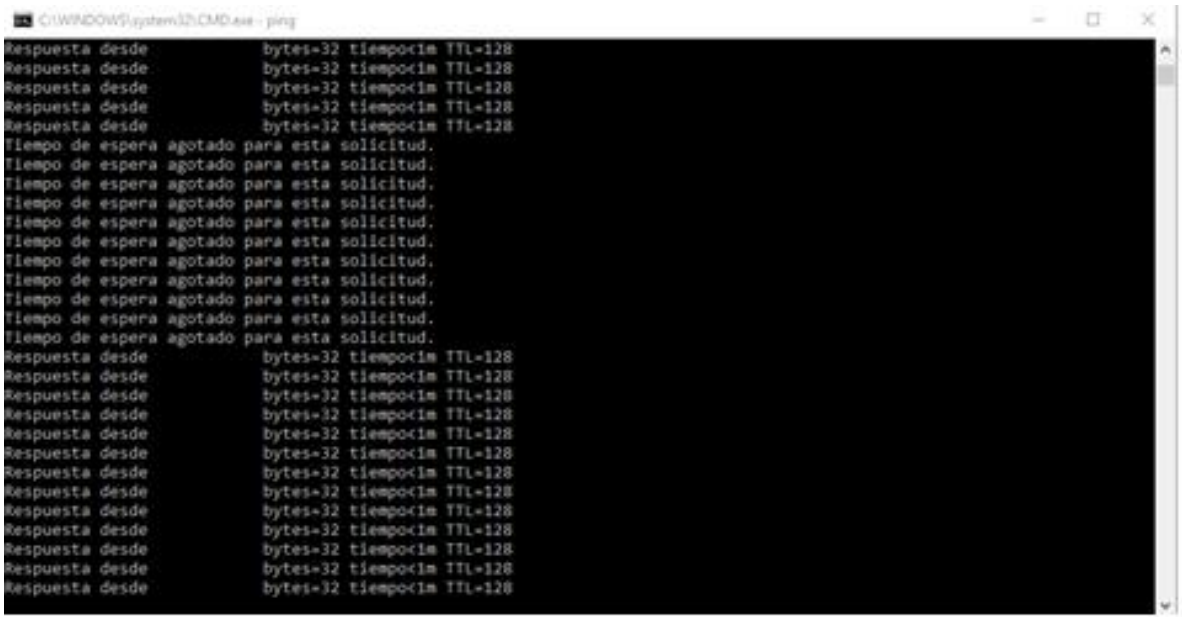
Figura 28 Bloqueo de paquetes protocolo *icmp* por el *Snort*



Fuente: El Autor

Para finalizar la prueba del *Snort IPS* se detiene el monitoreo de la consola y se observa la respuesta al ping por el host, dado que la consola del *IPS* se encuentra deshabilitada como se observa a continuación en la Figura 28.

Figura 29 Ping de respuestas del host con *Snort* desactivado

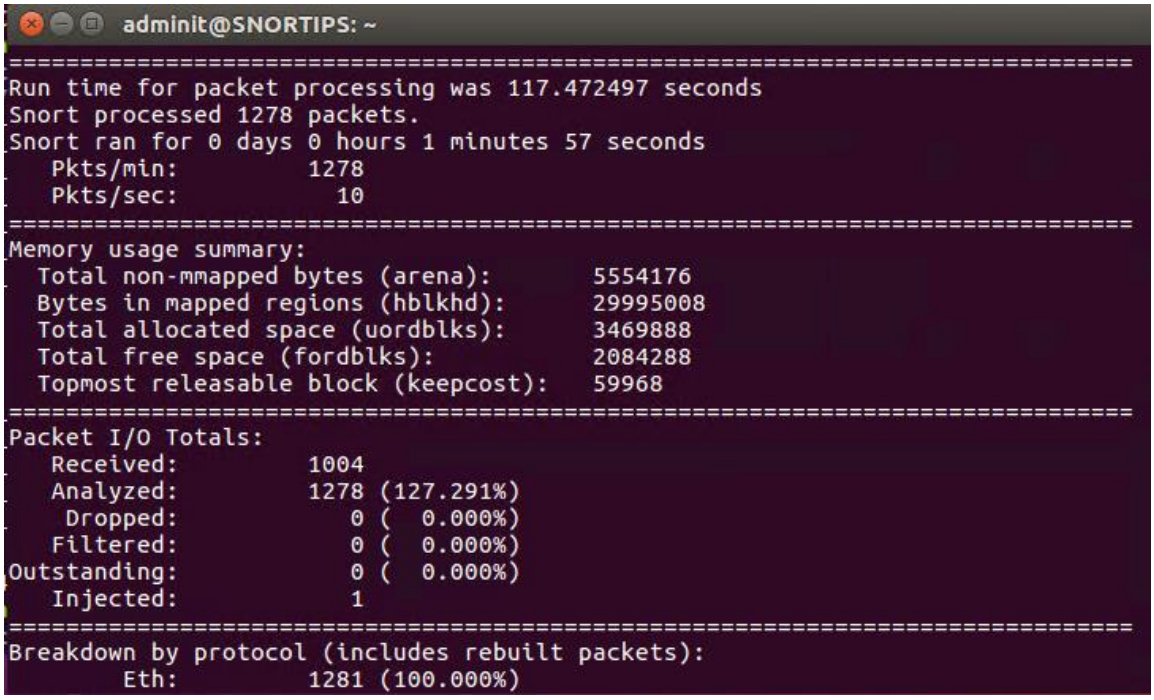


Fuente: El Autor

En la Figura 29 se puede observar la fortaleza que tiene el *Snort* para realizar bloqueo a nivel de protocolo, similar a un ataque cuando el intruso está dentro de nuestra red puede realizar este tipo de escaneos, estos sistemas no solo revisan las cabeceras de los paquetes, sino que también pueden analizar el contenido para validar que el tráfico no sea malicioso.

La Figura 30 muestra las estadísticas de los paquetes procesados por el *Snort* durante un periodo de 1 minuto y 57 segundos que se mantuvo activo el modo *Inline,* se analizaron 1278 paquetes, 1004 recibidos y uno rechazado.

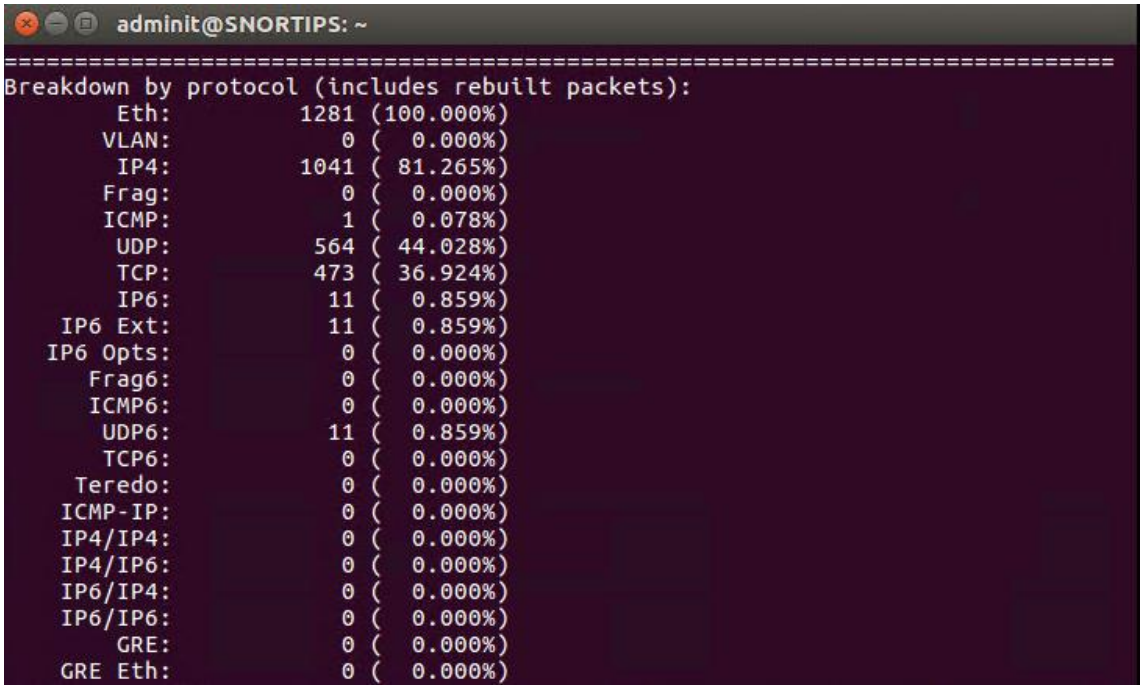
Figura 30 Resultado de Monitoreo del *Snort* por medio de consola



Fuente: El Autor

La Figura 31 muestra la clasificación por protocolos del tráfico analizado durante el periodo, el preprocesador se encarga de esta actividad y la pasa al módulo de detección para que tome la acción de acuerdo al cumplimiento de la regla.

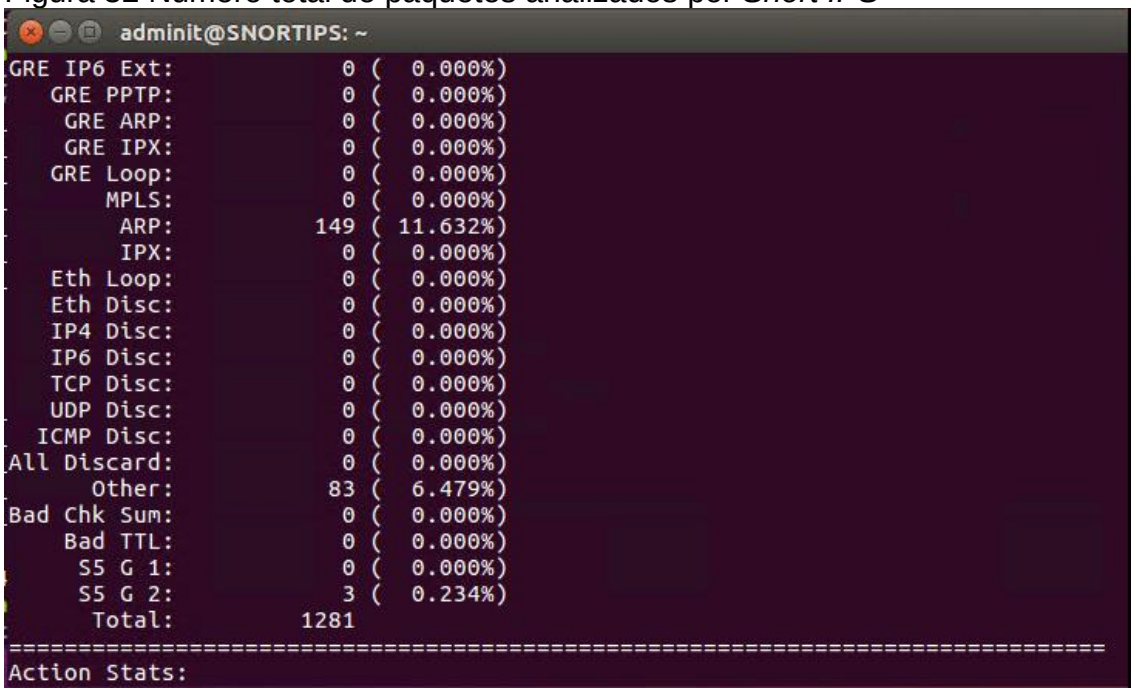
Figura 31 Resultado de paquetes detectado por protocolos



Fuente: El Autor

En total se analizaron 1281 paquetes durante el periodo de prueba, lo que demuestra la capacidad que tiene el *Snor*t de analizar tráfico y poder detectar algún comportamiento anormal directamente en la consola como se puede observar a continuación en la Figura 32.

Figura 32 Número total de paquetes analizados por *Snort IPS*



Fuente: El Autor

7.3.12 Instalación manual de reglas. Después de probado el modo *IPS* del *Snort* el paso que sigue es descargar las reglas desde el sitio oficial y descomprimirlas en el directorio del *Snort* para habilitarlas:

cd ~/snort_src

wget https://www.snort.org/reg-rules/snortrules-snapshot-29110.tar.gz/<SNORTCODE> -O snortrules-snapshot-29110.tar.gz

sudo tar xvfvz snortrules-snapshot-29110.tar.gz -C /etc/Snort

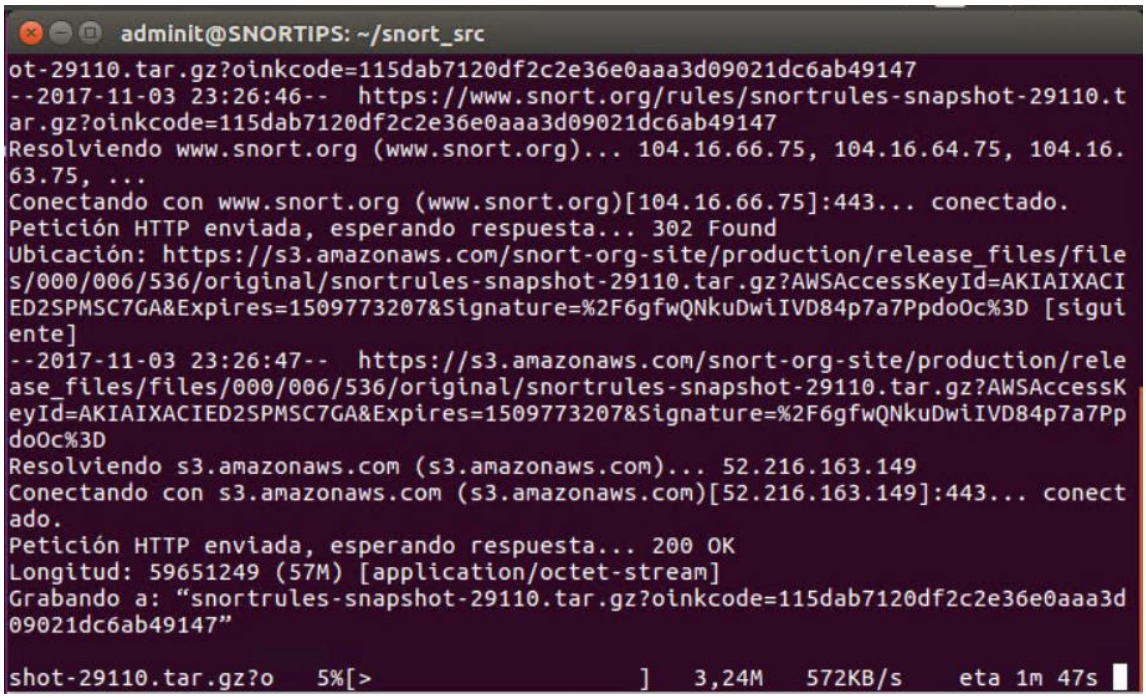
sudo cp ./.conf* ../*

sudo cp ./.map ../*

cd /etc/snort

sudo rm -Rf /etc/snort/etc

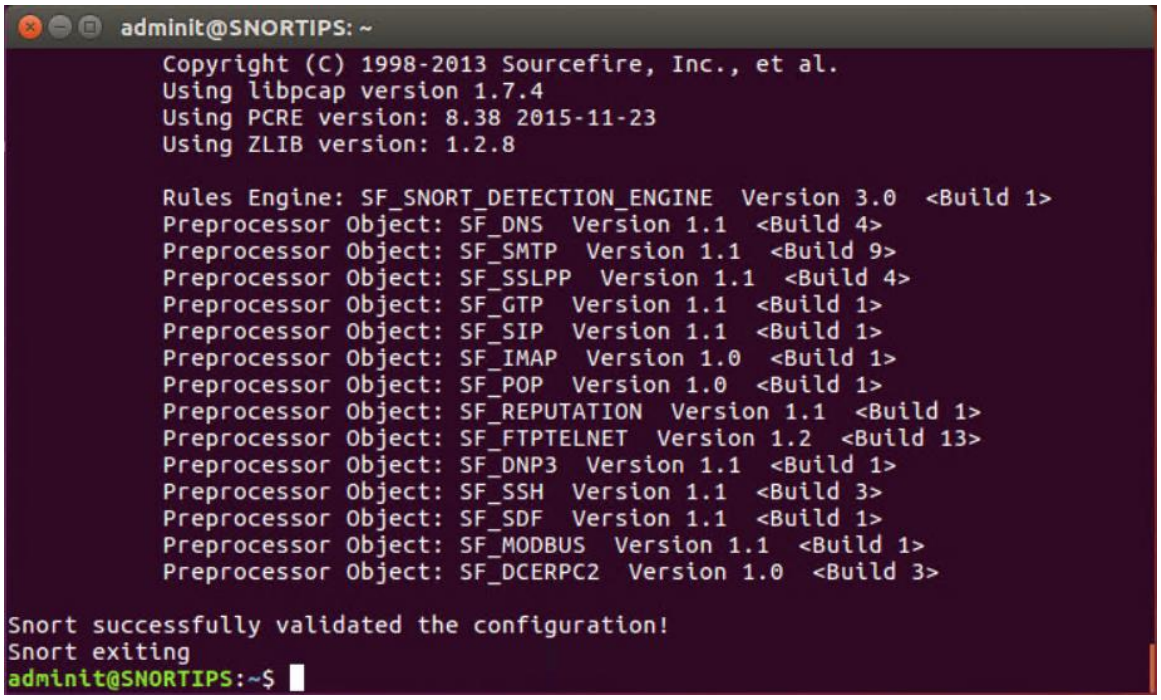
Figura 33 Descarga de reglas del *Snort*



Fuente: El Autor

Se procede con las descargas de las reglas desde el sitio oficial del *Snort* , el paso que sigue es la comprobación de la configuración del *Snort* con las reglas actualizadas para luego realizar el test de validación como se muestra a continuación en La figura 34.

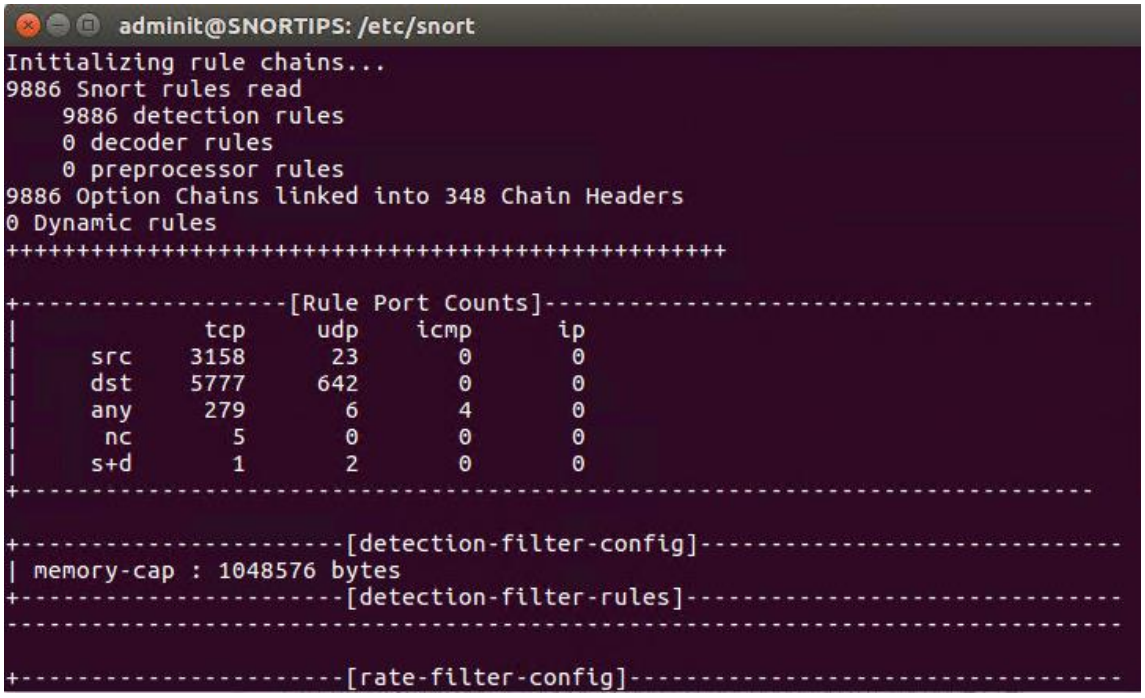
Figura 34 Validando de reglas descargadas desde el sitio oficial del *Snort*



Fuente: El Autor

La Figura 34 muestra que el snort detectó que tiene instaladas 9.886 reglas, las cuales se descargaron directamente desde el sitio web y se descomprimieron en el directorio /etc/snort/rules. Con esta configuración el *IPS* queda habilitado para operar y detectar cualquier intento de intrusión.

Figura 35 Reglas detectadas por el *Snort*



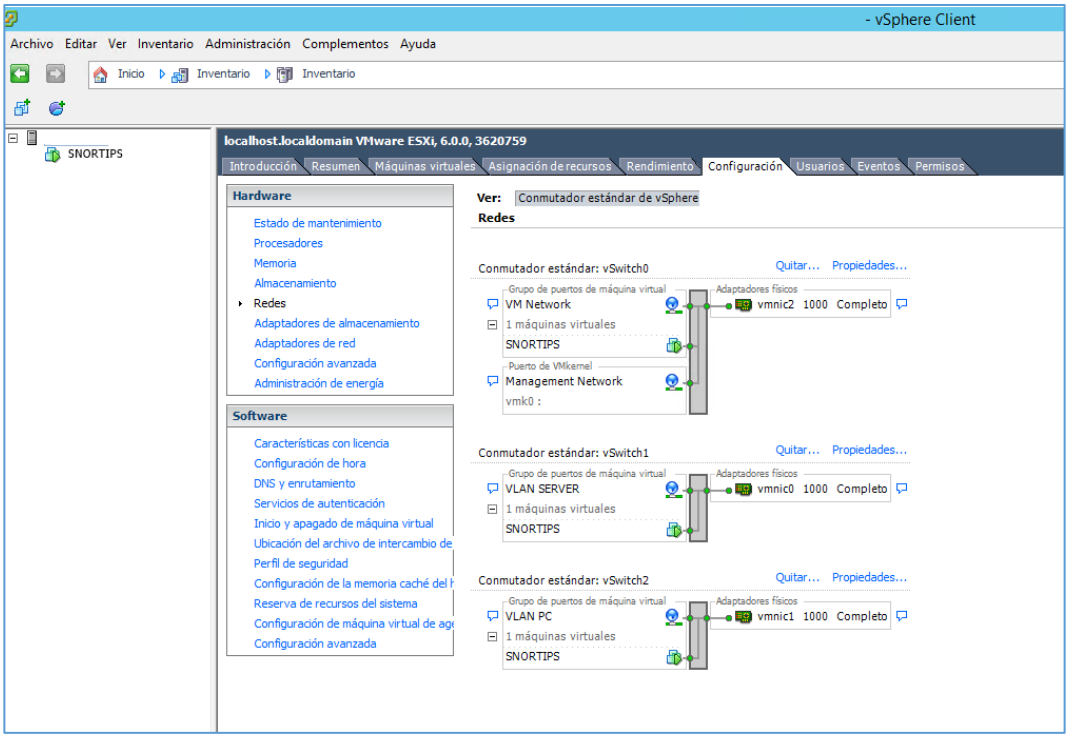
Fuente: El Autor

RESULTADOS Y DISCUSION

Se realizó un levantamiento de información que permitió conocer la infraestructura de servidores y equipos de comunicaciones de la sede de Bucaramanga, la red de datos se encuentra segmenta en redes lógicas o *Vlan*. La empresa adquirió un sistema de seguridad perimetral de última generación que combina las características de *Firewall/IPS*, este sistema utiliza reglas de Snort que actualiza de manera automática. Sin embargo, a pesar de que este sistema tiene control sobre la red local, se debe reforzar la seguridad en la *Vlan* de servidores.

Por esta razón, se definió que el Snort debería ubicarse en la red Interna. Se constató con la herramienta *nmap* que se puede realizar escaneos de puertos y servicios en esa red y pasar desapercibido. Se diseño un sistema de Prevención de Intrusos utilizando la arquitectura de Snort en un ambiente virtualizado en *Vmware Esxi* detrás del F*irewall* como se evidencia en la Figura 37.

Figura 36 *VM Snort IPS* en *Host VMware ESXi 6.0*

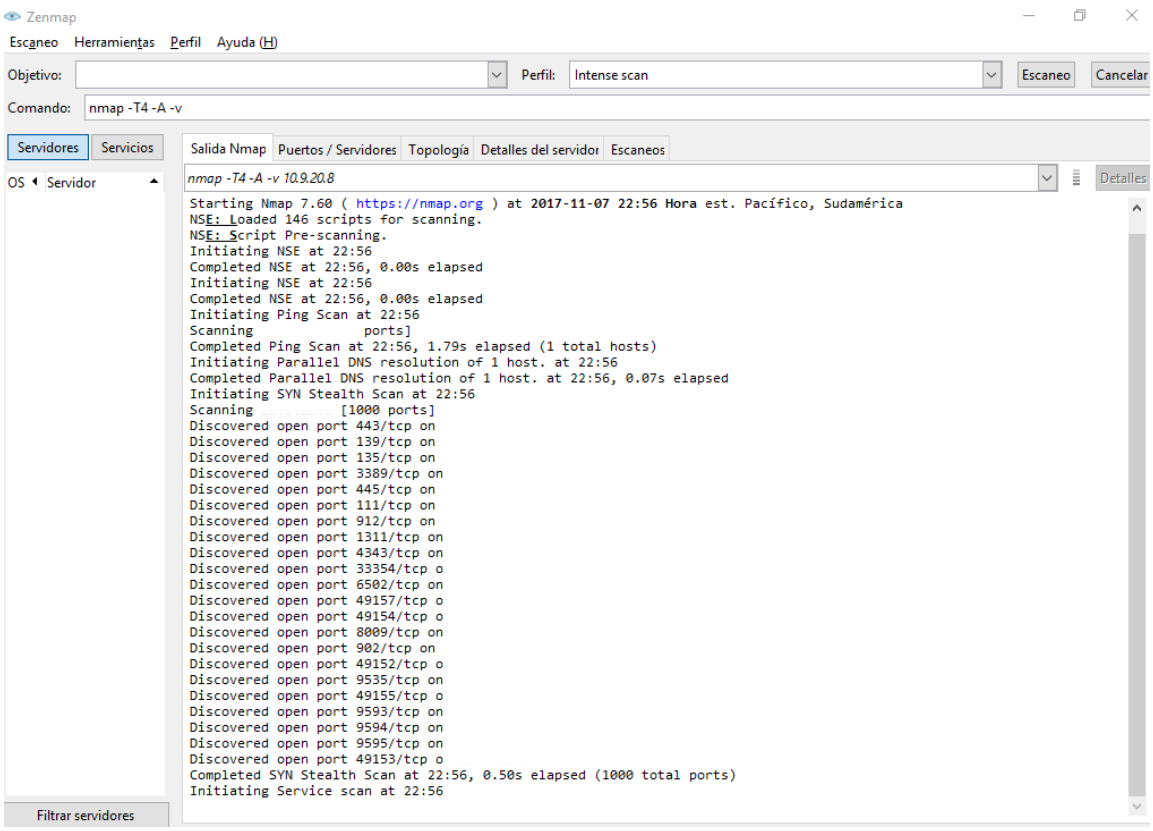


Fuente: El Autor

Con este proyecto se fortaleció el mecanismo de protección en la *Vlan* de Servidores de la empresa Minesa, este sistema refuerza la seguridad en el segmento de red de datos de los Servidores, inspecciona el tráfico y bloquea los paquetes por medio del motor de detección utilizando las reglas activas. También, ayuda a prevenir el escaneo no autorizado a puertos que ofrecen servicios en la red impidiendo que las vulnerabilidades en los servidores sean detectadas y explotadas. Se realizaron escaneos a los servidores con *nmap* que antes no era posible detectarlos, se constató la efectividad del sistema en el bloqueo de un ataque de escaneo sobre un host dentro de la red protegida. Con este sistema se tendría un filtrado a nivel de protocolos con un nivel de detalle de la *IP* y Puerto origen que envía el tráfico malicioso. Como prueba de lo mencionado, se realiza un escaneo a un servidor dentro de la red protegida, en la Figura 37 se evidencia la enumeración de los

puertos *TCP* abiertos con cada uno de los servicios asociados, esto representa una vulnerabilidad dado que el escaneo de puertos hace parte de las fases preliminares de un ataque, lo que representa un riesgo alto si un atacante logra ingresar a la red interna utilizando alguna técnica de ingeniería social puede dejar instalado un *Sniffer* para interceptar el tráfico en ese segmento de red. También, se reforzó la capacidad de prevención de intrusiones en la red local que combinado al sistema de seguridad perimetral generan una capa de seguridad en la red de servidores.

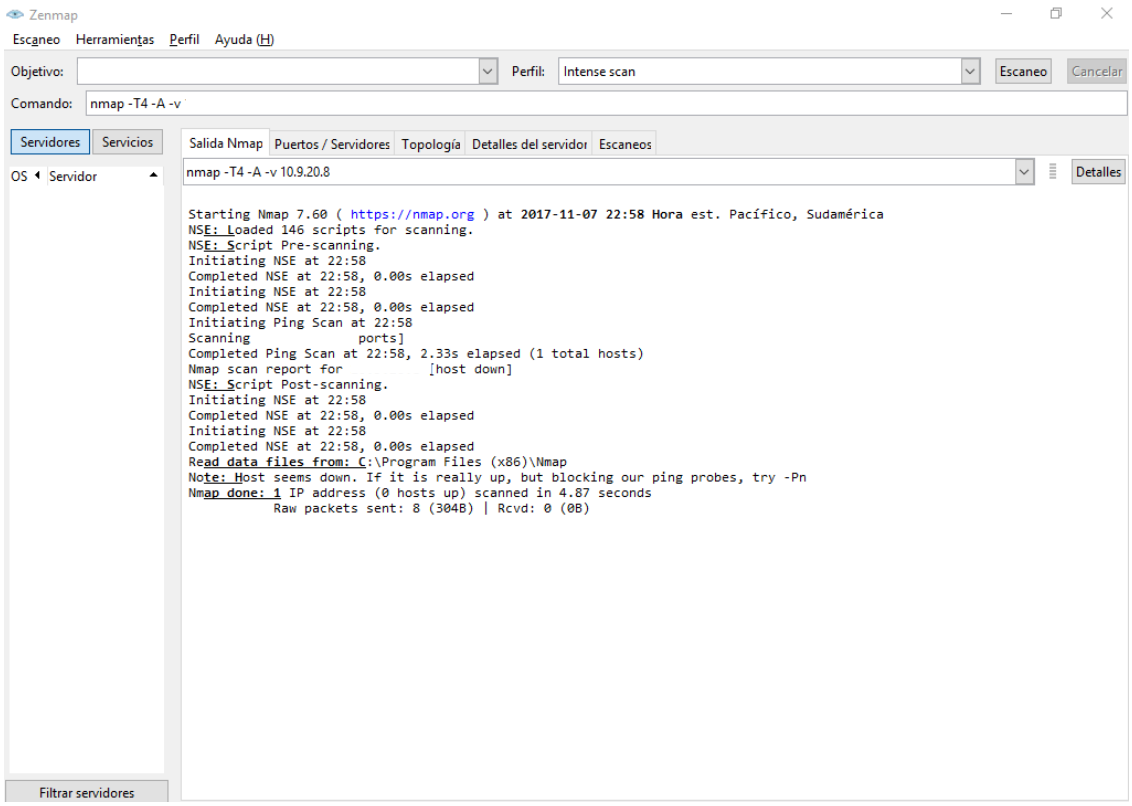
Figura 37 Resultado de Escaneo con *nmap*



Fuente: El Autor

Se ejecuta nuevamente el escaneo con *nmap* al mismo host con el *Snort* en modo *IPS*, en la Figura 38 se evidencia el bloqueo del escaneo, lo que justifica la instalación de esta capa de protección en la Vlan de servidores.

Figura 38 Bloqueo de Ping por el Snort

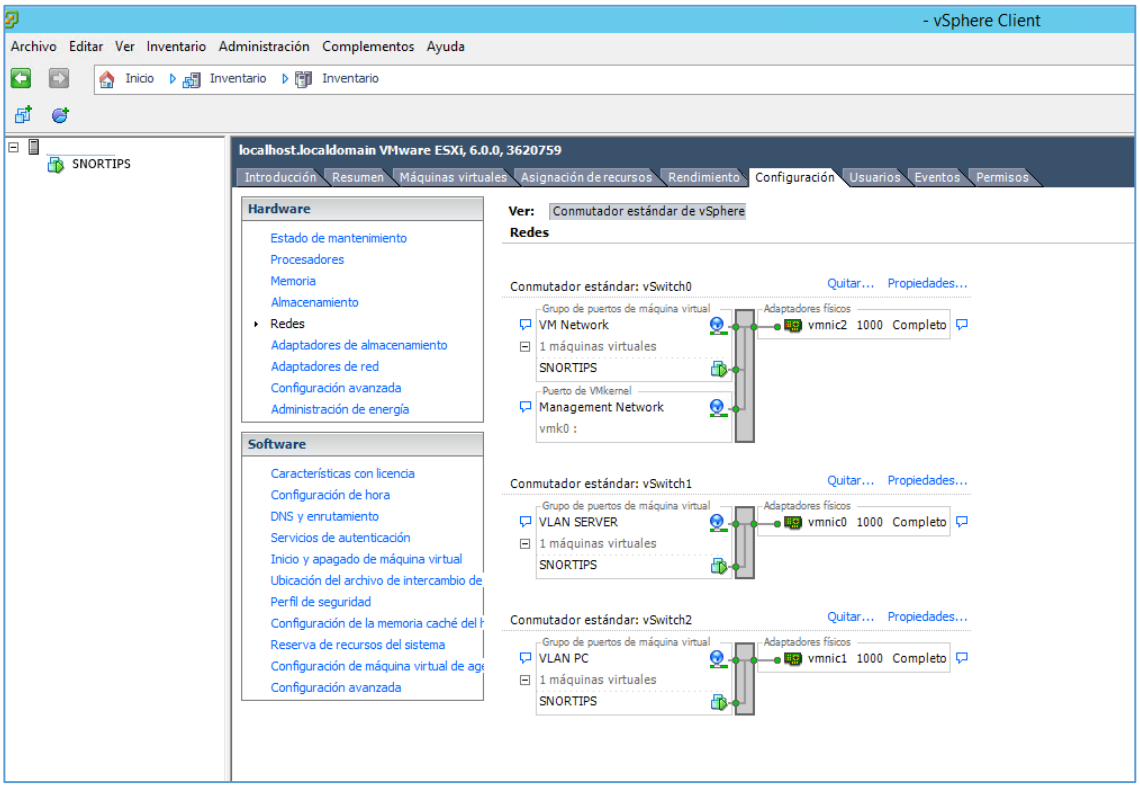


Fuente: El Autor

La instalación de *Snort IPS* se hizo en un entorno completamente virtualizado en *VMware*, con tres (3) Interfaces de Red físicas y Tres (3) *Virtual Switch*; el *VSwitch0* con interfaz de red para gestión de la Máquina Virtual, el *VSwitch1* y *VSwitch2* funciona en modo promiscuo, permitiendo la captura del tráfico sirviendo de puente entre el tráfico que pasa de la *Vlan* de PC a la Vlan de Servidores, realizando un

bloqueo de los paquetes que contengan algún patrón de ataque que coincida con una de las reglas.

Figura 39 *VM Snort IPS* en *Host VMware ESXi 6.0*



Fuente: El Autor

RECOMENDACIONES

- El sistema inicialmente se mantendrá monitoreado para evitar bloqueos en el ambiente de producción hasta lograr estabilizarlo hasta minimizar el número de falsos positivos, con esto se podrá realizar ajustes en su configuración para mejorar su desempeño.

- Realizar pruebas al sistema con las herramientas de *Pentest* inyectando tráfico de paquetes y alteración del protocolo en el encabezado de los paquetes para mejorar su capacidad de detección.

- Aplicar actualizaciones y parches de seguridad.

DIVULGACION

La Divulgación del proyecto se hará dentro de los repositorios de La Universidad Nacional Abierta y a Distancia como proyecto aplicado de un Sistema de Prevención de Intrusos bajo la plataforma *Linux Ubuntu 16.04*, el aporte se genera en este sentido las guías son incompletas sobre la implementación del *Snort* como *IPS* en Sistema Operativo Linux.

BIBLIOGRAFIA

ATAQUES INFORMÁTICOS EN COLOMBIA Y SECTORES MÁS AFECTADOS. En línea 11 de septiembre de 2016 disponible en http://www.vanguardia.com/actualidad/colombia/250540-98-de-empresas-colombianas-son-victimas-de-ataques-informaticos

ESCRIVÁ GASCÓ, Gema; ROMERO SERRANO, Rosa Maria y RAMADA, David Jorge y ONRUBIA PEREZ, Ramón. Seguridad Informática,
Málaga: Macmillan, 2013. P. 7

FACULTAD DE CIENCIAS EXACTAS, Protocolo OSI. En línea. Fecha. 13 septiembre de 2016 disponible en: http://www.exa.unicen.edu.ar

GOMEZ LOPEZ, Julio. Optimización de Sistemas de Detección de Intrusos en Red Utilizando Técnicas Computacionales Avanzadas. Barcelona, 2009. Universidad de Almería. Facultad de Informática. Informática.

INSTALACIÓN SNORT 2.9 EN UBUNTU 16. En Línea. Fecha. 7 Mayo de 2017 disponible en: https://www.snort.org/documents/snort-3-on-ubuntu-14-and-16

LEY 1273 DE 2009. En línea. Fecha. 31 agosto de 2016 disponible en: http://www.redipd.org/legislacion/common/legislacion/Colombia/ley_1273_05012009_Colombia.pdf

RED HAT ENTERPRISE LINUX 4 MANUAL DE SEGURIDAD. En línea. Fecha. 20 octubre de 2016 disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html

REVISTA DEL INSTITUTO TECNOLÓGICO DE INFORMÁTICA. En línea. Fecha. 25 octubre de 2016 disponible en: http://web.iti.upv.es/actualidadtic/2005/02/2005-02-intrusos.pdf

SALAZAR MORALES, Jorge Iván, Seguridad Avanzada en Redes de Datos. Medellín: 2013, 171p. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática.

SANTOS COSTAS, Jesus, Seguridad Informática.
Madrid: MacMillan. 2013. 216p.

SISTEMA DE PREVENCIÓN DE INTRUSOS. En línea. Fecha. 11 septiembre de 2016 disponible en: https://www.ecured.cu/Intrusion_Prevention_System

STALLINGS, William, Fundamentos de Seguridad en Redes Aplicaciones y Estándares. 2da Edición. Madrid: Pearson Educación, 2004. 418p.

SNORT IPS DAQ AFPACKET. En Línea. Fecha. 2 Abril de 2017 disponible en: https://www.snort.org/documents/snort-ips-using-daq-afpacket

VIEITES GOMEZ, Álvaro, Seguridad en Equipos Informáticos.
Madrid: Starbook Editorial. 2014. 168p

ANEXOS

ANEXO A Carta Formal de Aprobación del Proyecto

Bucaramanga, noviembre 16 de 2017

ACTA DE ACEPTACION Y RECIBO A SATISFACION

Por medio de la presente hacemos constar que el señor RAFAEL LUIS MOSCOTE MEDINA, desarrollo su proyecto de grado titulado SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS IPS PARA LA VLAN DE SERVIDORES DE LA SOCIEDAD MINERA DE SANTANDER S.A.S. EN BUCARAMANGA (SANTANDER), se documentó la instalación y puesta en marcha del Sistema Snort IPS/IDS en una ambiente de producción virtualizado en VMware Esxi 6.0, da solución al problema de intrusiones en la Vlan de servidores, se realizaron pruebas de bloqueo de escaneos ping y nmap, autorizando la entrega a la Universidad Abierta y A Distancia y al programa Ciencias Básicas Tecnología e Ingeniería las evidencias del trabajo realizado para optar al título de especialista en seguridad informática.

Agradeciendo su atención y reiterando nuestra conformidad con el trabajo realizado

Atentamente,

ANDERSON RIVERA
Gerente de TI

16/11/2017

Transversal Oriental 90 – 10.2 Torre Empresarial Parque Real 33 • Bucaramanga, Santander • Colombia • 57 7 6971300 •

ANEXO B. Correo de Aprobación del Proyecto

Rafael Luis Moscote Medina

De: Andres Calderon
Enviado el: martes, 15 de noviembre de 2016 3:35 p.m.
Para: Anderson Rivera Rivera; Eduardo Enrique Mayorga Rojas; Floralba Menjura Jara; Luis Guillermo La Rotta C.; Jorge Gonzalez
CC: Rafael Luis Moscote Medina
Asunto: RE: Solicitud de información

Efectivamente, excelente Rafa.

Estamos pendientes a ver cómo podemos colaborar en el proyecto.

Saludos

De: Anderson Rivera Rivera
Enviado el: martes, 15 de noviembre de 2016 08:29 a.m.
Para: Andres Calderon <andres.calderon@minesa.com>; Eduardo Enrique Mayorga Rojas <eduardo.mayorga@minesa.com>; Floralba Menjura Jara <floralba.menjura@minesa.com>; Luis Guillermo La Rotta C. <luis.larotta@minesa.com>; Jorge Gonzalez <jorge.gonzalez@minesa.com>
CC: Rafael Luis Moscote Medina <rafael.moscote@minesa.com>
Asunto: FW: Solicitud de información

Rafa,

Excelente iniciativa y cuenta con el área de IT para ayudarte en lo que sea posible.

Finance Team,

Quisiera compartirles ésta iniciativa de Rafa la cual traerá un beneficio a la compañía en términos de protección contra ataques cibernéticos (actualmente vulnerables) y lo más importante, que servirá como tesis de su proyecto de grado de la especialización.

Saludos,


Anderson Rivera Rivera
Gerente TI | IT Manager

Bucaramanga - Colombia
Transversal Oriental 90 - 102 Piso 11
Torre Empresarial Cacique | 680001
t +57 7 6971200 Ext. 1138
c +57 3214610602
anderson.rivera@minesa.com

From: Rafael Luis Moscote Medina
Sent: Monday, November 14, 2016 11:04 PM
To: Departamento de TI <soporte_TI@minesa.com>
Subject: Solicitud de información

1

ANEXO C Correo de Solicitud de Aval del Proyecto

Buenas noches Estimados,

Les comparto información del Anteproyecto que actualmente estoy desarrollado como requisito de grado en la Universidad, y a la vez contar con su valiosa colaboración respondiendo el siguiente cuestionario:
https://docs.google.com/forms/d/1pWTnTkjD-ApTsYdNp6GBfOXq4_FlMI3pUG-Iu0keRuU/edit

4. OBJETIVOS DEL PROYECTO

4.1 OBJETIVO GENERAL

Instalar un sistema de detección y prevención de intrusos, utilizando la arquitectura del *Snort*, como mecanismo para fortalecer la seguridad en la *VLAN* de servidores de la Sociedad Minera de Santander S.A.S. en Bucaramanga (Santander).

4.2 OBJETIVOS ESPECÍFICOS

- Recopilar información del esquema de seguridad de la *VLAN* de servidores de la Empresa Minesa S.A.S, utilizando técnicas de recolección de datos para conocer el nivel de protección.

- Diseñar un esquema de red utilizando *IPS* detrás del firewall que permita monitorear el tráfico que entra a la *VLAN* de servidores para detectar intentos de ataque y fortalecer la seguridad de la red local de la Empresa Minesa S.A.S

- Instalar el sistema de seguridad con la herramienta *IPS* para bloquear las vulnerabilidades y amenazas que presenta *VLAN* de servidores de la Empresa Minesa S.A.S

Mil gracias por su colaboracion.

Cordial & Atentamente,

Rafael Luis Moscote Medina
Departamento IT
Minesa
t+57 6971217 Ext 1217
Cel: 3209267875
Email: rafael.moscote@minesa.com

ANEXO D Cuestionario

Sociedad Minera de Santander S.A.S.

Minesa

CUESTIONARIO

Objetivo: Recolectar información sobre las necesidades y requerimientos de implementación de un Sistema de Prevención de Intrusos IPS para el fortalecimiento de la seguridad en la red datos de la Empresa MinesaS.A.S.

Por favor lea las preguntas y marque con una X su respuesta.

1. ¿Considera usted que el nivel de seguridad informático que actualmente tiene la red de datos de Minesa es?

- ◯ Alto
- ◯ Medio
- ◯ Bajo
- ◯ Other: _____

2. ¿Cree usted que se debe fortalecer el actual sistema de seguridad informática en la red de Minesa?

- ◯ Si
- ◯ No
- ◯ No responde
- ◯ Other: _____

3. ¿Conoce usted que es un Ataque informático?

- ◯ Si
- ◯ No
- ◯ Other:

4. ¿Los Equipos que ofrecen seguridad en la red son actualizados con frecuencia?

- ◯ Si
- ◯ No
- ◯ No responde
- ◯ Other: _____

5. ¿Identifica un ataque a la red de datos?

- ◯ Si
- ◯ No
- ◯ No Responde
- ◯ Other: _____

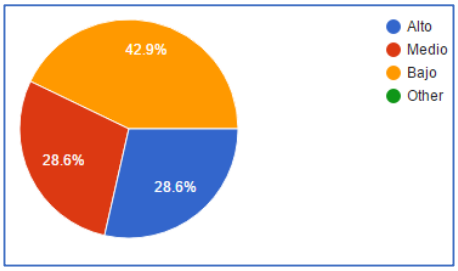
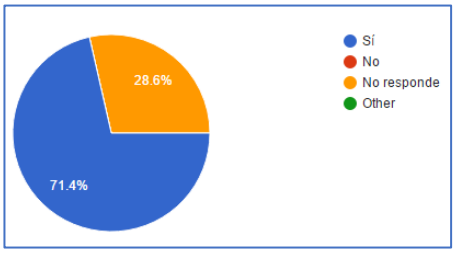
6. ¿Se tiene definido un plan de contigencia en caso de ocurrir algún ataque a la red?.

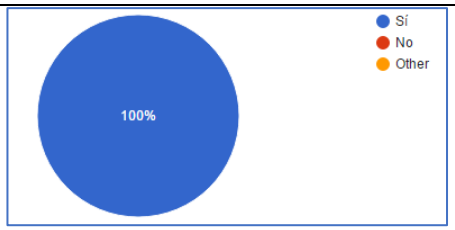
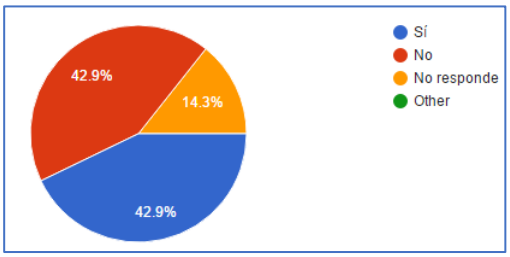
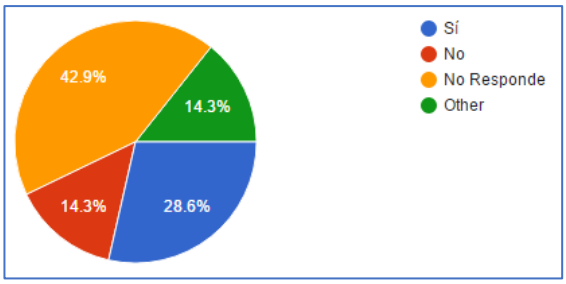
- ◯ Si
- ◯ No
- ◯ Other: _____

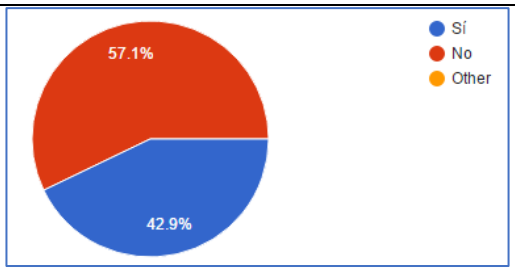
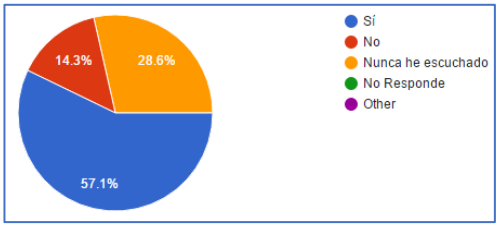
7. ¿Conoce que es un Sistema de Prevención de Intrusos IPS?

- ◯ Si
- ◯ No
- ◯ Nunca he escuchado
- ◯ No Responde
- ◯ Other: _____

ANEXO E Resultado y Análisis de Encuesta

N	Preguntas	Respuestas	Análisis
1	¿Considera usted que el nivel de seguridad informático que actualmente tiene la red de datos de Minesa es?	Alto, Medio, Bajo Otro	El 42.9 % de los integrantes del Departamento de TI opinan que el nivel de seguridad en la red de datos necesita ser reforzado con mecanismos que permitan hacer monitoreos en tiempo real. 
2	¿Cree usted que se debe fortalecer el actual sistema de seguridad informática en la red de Minesa?	Si No, Nunca he escuchado No Responde Otro	La mayoría de los profesionales de IT de Minesa opinan que se debe fortalecer el actual esquema de seguridad de la red, por sistemas más robustos que permitan detectar anomalías o acceso no autorizados a la red. 
3	¿Conoce usted que es un Ataque informático?	Si, No, Nunca he escuchado	Se puede observar que la totalidad de los integrantes del Departamento de TI conocen que es un ataque informático, puede ser que algunos lo han escuchado en noticia, o leído en internet, pero hasta el momento no lo han experimentado.

		No Responde, Otro	
4	¿Los Equipos que ofrecen seguridad en la red son actualizados con frecuencia?		La mitad de los integrantes del Departamento de TI afirman que los equipos son actualizados, la otra mitad no. No se tiene definida una política para la actualización periódica de los equipos y planes de backup. 
5	¿Identifica un ataque a la red de datos?	Si, No, Nunca he escuchado No Responde, Otro	La mayoría responden que no identifica un ataque a la red de datos, no se cuenta con herramientas que permitan generar estadísticas o reportes que lo certifiquen. 
6	¿Se tiene definido un plan de contingencia en caso de ocurrir algún	Si, No, Nunca he escuchado No Responde, Otro	En grafico se muestra que la mayoría respondieron que no se tiene un plan de contingencia documentado y procedimientos a seguir en el caso que ocurra un ataque que coloque en riesgo los sistemas informáticos y redes de la empresa.

	ataque a la red?		
7	¿Conoce que es un Sistema de Prevención de Intrusos IPS?	Si, No, Nunca he escuchado No Responde, Otro	La mitad de los encuestados conocen que es un IPS. Sin embargo, la empresa no cuenta con uno que le permita fortalecer su seguridad, que le envíe alertas automáticamente en el momento que la red sea objeto de un escaneo de puertos y servicios. 

ANEXO F Resumen Analítico Especializado – RAE

Resumen Analítico Especializado - RAE	
1. Titulo	SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS IPS PARA VLAN DE SERVIDORES DE LA SOCIEDAD MINERA DE SANTANDER S.A.S. EN BUCARAMANGA (SANTANDER).
2. Autor	Rafael Luis Moscote Medina
3. Edición	2017
4. Fecha	Diciembre 12 de 2017
5. Palabra Claves	Sistema de Detección y Prevención de Intrusos, Modelo *OSI*, *Hacking* Ético, *TCP*, *UDP*, *ICMP*, *IP*, Ataque, *nmap*, Vulnerabilidad, Snort, Regla, Puerto, Alerta, Tráfico, *DAQ*, *Inline*.
6. Descripción	
Proyecto de Grado Aplicado para Optar al Título de Especialista en Seguridad Informática, consiste en la instalación de un Sistema de detección y prevención de intrusos basado en red para la Sociedad Minera de Santander S.A.S en Bucaramanga (Santander), este sistema permite el análisis del tráfico en tiempo real que ingresa a la *Vlan* de Servidores en búsqueda de posible ataques y anomalías en las cabeceras de paquetes y protocolos de la capa de red (*IP*, *UDP, TCP e ICMP*) utiliza un lenguaje de reglas para detección y bloqueo de intrusiones, realizando un análisis de protocolos con información de la IP de donde se originó el ataque y hacia que destino y puerto.	
7. Fuentes	

ATAQUES INFORMÁTICOS EN COLOMBIA Y SECTORES MÁS AFECTADOS. En línea 11 de septiembre de 2016 disponible en http://www.vanguardia.com/actualidad/colombia/250540-98-de-empresas-colombianas-son-victimas-de-ataques-informaticos

ESCRIVÁ GASCÓ, Gema; ROMERO SERRANO, Rosa Maria y RAMADA, David Jorge y ONRUBIA PEREZ, Ramón. Seguridad Informática,
Málaga: Macmillan, 2013. P. 7

FACULTAD DE CIENCIAS EXACTAS, Protocolo OSI. En línea. Fecha. 13 septiembre de 2016 disponible en: http://www.exa.unicen.edu.ar

GOMEZ LOPEZ, Julio. Optimización de Sistemas de Detección de Intrusos en Red Utilizando Técnicas Computacionales Avanzadas. Barcelona, 2009. Universidad de Almería. Facultad de Informática. Informática.

INSTALACIÓN SNORT 2.9 EN UBUNTU 16. En Línea. Fecha. 7 Mayo de 2017 disponible en: https://www.snort.org/documents/snort-3-on-ubuntu-14-and-16

LEY 1273 DE 2009. En línea. Fecha. 31 agosto de 2016 disponible en: http://www.redipd.org/legislacion/common/legislacion/Colombia/ley_1273_05012009_Colombia.pdf

RED HAT ENTERPRISE LINUX 4 MANUAL DE SEGURIDAD. En línea. Fecha. 20 octubre de 2016 disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html

REVISTA DEL INSTITUTO TECNOLÓGICO DE INFORMÁTICA. En línea. Fecha. 25 octubre de 2016 disponible en: http://web.iti.upv.es/actualidadtic/2005/02/2005-02-intrusos.pdf

SALAZAR MORALES, Jorge Iván, Seguridad Avanzada en Redes de Datos. Medellín: 2013, 171p. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática.

SANTOS COSTAS, Jesus, Seguridad Informática.
Madrid: MacMillan. 2013. 216p.

SISTEMA DE PREVENCIÓN DE INTRUSOS. En línea. Fecha. 11 septiembre de 2016 disponible en: https://www.ecured.cu/Intrusion_Prevention_System

STALLINGS, William, Fundamentos de Seguridad en Redes Aplicaciones y Estándares. 2da Edición. Madrid: Pearson Educación, 2004. 418p.

SNORT IPS DAQ AFPACKET. En Línea. Fecha. 2 Abril de 2017 disponible en: https://www.snort.org/documents/snort-ips-using-daq-afpacket

VIEITES GOMEZ, Álvaro, Seguridad en Equipos Informáticos.
Madrid: Starbook Editorial. 2014. 168p.

8. Contenidos

El documento inicia con una introducción sobre la importancia de la implementación de sistemas detección y prevención de intrusiones en una red y la problemática actual de seguridad, en donde la mayoría de los ataques se presentan al interior de las organizaciones y que muchas veces no son detectadas por los cortafuegos. Luego, se describe el problema estudio y los objetivos que

ayudaron a enmarcar el contexto sobre el cual se desarrolló el proyecto. El plan del proyecto inicia con un análisis del esquema de seguridad actual, seguido se propone un nuevo diseño de red que incluya un sistema de detección y prevención de intrusos, se instala y se realizan pruebas. Finalmente, se evalúa la efectividad de la herramienta en el bloqueo de intrusiones.

9. Metodología

Para la elaboración de este proyecto fue necesario aplicar la metodología investigativa conocer el estado del arte de los sistemas de detección y prevención de intrusos, luego se recopila la información del esquema de red actual de la empresa y se propone una nueva topología que incluya un IPS detrás del Firewall, teniendo en cuenta que la mayoría de los ataques que se producen en una red son internos, se realizan pruebas y se valida su correcto funcionamiento.

10. Conclusiones

Con este proyecto se fortaleció el mecanismo de seguridad en la red de datos de la empresa Minesa, se comprobó que no cuenta con un sistema de detección de intrusiones a nivel interno de su red de servidores que permita descubrir y bloquear acciones y alertar de comportamientos anómalos a nivel interno. También, ayudó a prevenir el escaneo no autorizado a puertos de los servidores y facilitó la remediación de problemas de seguridad interno y en la definición de políticas que garanticen la confidencialidad, disponibilidad e integridad de la información.

11. Recomendaciones

- El sistema inicialmente se mantendrá monitoreado para evitar bloqueos en el ambiente de producción hasta lograr estabilizarlo hasta minimizar el número de falsos positivos, con esto se podrá realizar ajustes en su configuración para mejorar su desempeño.

- Realizar pruebas al sistema con las herramientas de *Pentest* inyectando tráfico de paquetes y alteración del protocolo en el encabezado de los paquetes para mejorar su capacidad de detección.

• Aplicar periódicamente actualizaciones de reglas y parches de seguridad.	
12. Autor del RAE	Rafael Luis Moscote Medina