IMPLEMENTACIÓN DE UN IDS/IPS EN LA EMPRESA TRANSPORTES TMC S.A.S, USANDO UBUNTU LINUX

CESAR ENRIQUE SILVA GARCIA

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
FACULTAD DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VILLAVICENCIO
2017

IMPLEMENTACIÓN DE UN IDS/IPS EN LA EMPRESA TRANSPORTES TMC S.A.S, USANDO UBUNTU LINUX

CESAR ENRIQUE SILVA GARCIA

Proyecto aplicado para optar el título de Especialista en Seguridad Informática

Ing. Juan José Cruz Garzón
Director de Proyecto Ingeniería

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
FACULTAD DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VILLAVICENCIO
2017

CONTENIDO

Pág.

INTRODUCCIÓN 1

1. TITULO 2

2. DEFINICIÓN DEL PROBLEMA 3

2.1. ANTECEDENTES DEL PROBLEMA 3

2.2. FORMULACIÓN DEL PROBLEMA 3

2.3. DESCRIPCIÓN DEL PROBLEMA 3

3. JUSTIFICACIÓN 4

4. OBJETIVOS DEL PROYECTO 5

4.1. OBJETIVO GENERAL 5

4.2. OBJETIVOS ESPECÍFICOS 5

5. ALCANCE Y DELIMITACIÓN DEL PROYECTO 6

6. MARCO REFENCIAL 7

6.1. MARCO TEÓRICO 7

6.2. MARCO CONCEPTUAL 9

6.3. ESTADO DE ARTE 10

6.4. MARCO LEGAL 11

7. DISEÑO METODOLÓGICO 12

7.1. TIPO DE INVESTIGACIÓN 12

7.2. MÉTODOS DE INVESTIGACIÓN 12

7.2.1. FASES: 12

7.3. HIPÓTESIS 13
7.4. VARIABLES E INDICADORES 13
7.5. UNIVERSO 13
7.6. INSTRUMENTOS PARA LA RECOLECCIÓN DE INFORMACIÓN 13
8. ESQUEMA TEMÁTICO 15
8.1. LEVANTAMIENTO DE INFORMACIÓN DEL ESTADO ACTUAL DE TECNOLOGÍA Y SEGURIDAD, EVALUANDO LA SEGURIDAD INFORMÁTICA DE LA EMPRESA TRANSPORTES TMC 15
8.1.1. ESTADO ACTUAL DE LA TECNOLOGÍA 15
8.1.2. DIAGRAMA DE RED TRANSPORTES TMC 16
8.1.3. EVALUACIÓN DE LA SEGURIDAD TRANSPORTES TMC 17
8.2. DETERMINACIÓN DEL SISTEMA DE DETECCIÓN DE INTRUSOS QUE SE VA A IMPLEMENTAR PARA LA EMPRESA TRANSPORTES TMC S.A.S 19
8.2.1. EVALUACIÓN DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS 19
8.3. PRUEBAS DE CONFIABILIDAD IDS/IPS SNORT. 20
8.3.1. DIAGRAMA DE IMPLEMENTACIÓN 20
9. PROPONENTES DEL PROYECTO 21
9.1. PRIMARIOS 21
9.2. SECUNDARIOS 21
10. RECURSOS NECESARIOS PARA EL DESARROLLO 22
10.1. RECURSOS MATERIALES 22
10.2. RECURSOS INSTITUCIONALES 22
10.3. PRESUPUESTO 22

11. RESULTADOS E IMPACTOS ESPERADOS.....23
12. DIVULGACIÓN 24
13. CRONOGRAMA DE ACTIVIDADES.....25
14. CONCLUSIONES 26
15. RECOMENDACIONES.....27
16. BIBLIOGRAFÍA 28
ANEXOS.....29

LISTA DE TABLAS

Pág.

Tabla 1. Estado actual de la Tecnología.....15

Tabla 2. Elementos de Seguridad De la Empresa.....16

Tabla 3. Evaluación de Seguridad De la Empresa.....17

Tabla 4. Evaluación de Los Sistemas IDS/IPS.….....19

Tabla 5. Presupuesto…….....22

LISTA DE ANEXOS

Pág.

ANEXO A. Carta de aprobación instalación IDS/IPS Transportes TMC S.A.S…….....29

ANEXO B. Manual IDS/IPS Transportes TMC S.A.S.....30

ANEXO C. Formato Vulnerabilidades Encontradas, Transportes TMC S.A.S…....37

ANEXO D. Grafica Vulnerabilidades Encontradas, Transportes TMC S.A.S…....38

INTRODUCCIÓN

Cada minuto en el mundo aparecen nuevas vulnerabilidades diseñadas para afectar el correcto y continuo funcionamiento de las empresas, atacando el activo más importante que tienen que es la información, se puede tener múltiples herramienta de protección, como lo son antivirus, backups periódicos y documentados, servidores de dominio y firewall, pero aun teniendo los sistemas más avanzados de seguridad nunca estaremos ciento por ciento seguros, por eso es indispensable hacer seguimiento a las nuevas amenazas e intrusiones que pueden atacar nuestros sistemas de información a diario, para así determinar, puertos, programas y archivos que requieran más atención, y necesiten fortalecer e implementar nuevas técnicas de seguridad.

Los servidores IDS/IPS representan una solución fundamental en el momento de identificar y Generar alertas de eventos de seguridad, sobre todo en organizaciones que manejan un alto contenido de información, realizan transacciones virtuales y no se pueden permitir que su empresas se detengan de algún modo por los diferentes tipos de ataques que persiguen constantemente a nuestras empresas cada día, es imperativo estar a la vanguardia en seguridad y tecnología, mejorando, identificando y previniendo las debilidades en materia de infraestructura de sistemas de información, además de todo esto los servidores IDS/IPS permiten enfocaren el área la cual nuestra empresa necesita fortalecerse, para hacer las inversiones justas y adecuadas para el tamaño y requerimientos de la organización.

1. TITULO

IMPLEMENTACION DE UN IDS/IPS EN LA EMPRESA TRANSPORTES TMC S.A.S, USANDO UBUNTU LINUX.

AREA DE CONOCIMIENTO: Ingeniería

LINEA DE INVESTIGACION: Métodos de prevención de ataques informáticos mediante diferentes tipos de IDS /IPS

2. DEFINICIÓN DEL PROBLEMA

2.1. ANTECEDENTES DEL PROBLEMA

En el año 2002 EMILIO JOSE MIRA ALFARO, presenta trabajo de grado para adquirir el título de ingeniería informática, titulado “Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia”

En el año 2008 MARIA ISABEL GIMENEZ GARCIA, presenta trabajo de grado para adquirir el título de ingeniería informática, titulado “UTILIZACIÓN DE SISTEMAS DE DETECCIÓN DE INTRUSOS COMO ELEMENTO DE SEGURIDAD PERIMETRAL”

En el año 2013 CARLOS MANUEL FABUEL DÍAZ, presenta trabajo de grado para adquirir el título de ingeniero de telecomunicaciones, El proyecto de grado se titula “IMPLANTACION DE UN SISTEMA DE SEGURIDAD PERIMETRAL”

2.2. FORMULACIÓN DEL PROBLEMA

¿Cómo se puede evitar o disminuir los riesgos de la información expuesta a los diferentes ataques informáticos en los cuales se encuentra vulnerable la empresa transportes TMC S.A.S?

2.3. DESCRIPCIÓN DEL PROBLEMA

Según RSA Security en el 2015 el 94% de las empresas en el mundo reportaron ser víctimas de al menos un ataque informático, se presume que en Colombia se presentan aproximadamente 10 millones de ataques diarios, En la empresa transportes TMC S.A.S, estamos expuestos a Malware, Troyanos, Ramsomware, ataques de denegación de servicio, Pishing, Spam entre otros.

La empresa transportes TMC, ubicada en la ciudad de Villavicencio en el departamento del meta, dedicada al transporte de hidrocarburos, desde hace un año ha venido expandiendo su operación, manejando así volúmenes de información más altos, transacciones bancarias virtuales con mayor frecuencia y con mayores montos de dinero, además del incremento de usuarios cliente local y de acceso remoto. Se encuentra expuesta a numerosos y constantes ataques de diferentes tipos que puede afectar su continua operatividad.

3. JUSTIFICACIÓN

Este trabajo se realiza con el fin de determinar, identificar, analizar y prevenir los diferentes tipos de ataques a nivel de red que se puede presentar en la empresa transportes TMC S.A.S, los cuales pueden poner en riesgo la continua operatividad, confidencialidad, disponibilidad e integridad de la información, utilizando un computador con procesador Intel Celeron de 2.4 ghz, memoria Ram de 4G, disco duro de 512G, con la última actualización del sistema operativo Ubuntu server y la aplicación IDS/IPS Snort, realizando diferentes tipos de pruebas para establecer el correcto funcionamiento y operatividad de la herramienta.

Con un IDS/IPS implementado en la empresa transportes TMC S.A.S se podrá determinar el número de ataques que la empresa recibe a diario semanal o mensual, identificando los puertos y servidores más vulnerables con el objetivo de tomar las correcciones necesarias y pertinentes para evitar que alguno de estos ataques tengan éxito y cause así que la empresa pierda tiempo, dinero e incluso clientes, generando así seguridad en la manera que se realizan y se utilizan las diferentes transacciones y aplicaciones de manejo frecuente en la empresa, permitiendo un trabajo fluido y constante por los colaboradores de la organización, garantizando acceso a la información de manera rápida, eficiente y segura.

4. OBJETIVOS DEL PROYECTO

4.1. OBJETIVO GENERAL

Implementar un sistema de detección y prevención de intrusos para la empresa Transportes TMC S.A.S, utilizando Ubuntu Linux.

4.2. OBJETIVOS ESPECÍFICOS

1. Realizar el levantamiento de información del estado actual de los elementos de tecnología y seguridad, evaluando la seguridad informática de la empresa Transportes TMC.

2. Determinar el sistema de detección de intrusos, que se va a implementar en la empresa transportes TMC.

3. Desarrollar diferentes tipos de pruebas para verificar confiabilidad de la puesta en marcha del servidor IDS/IPS.

4. Elaborar la correspondiente documentación del IDS/IPS, como Manual de funcionamiento del IDS/IPS Snort, documento sobre las alertas de eventos de seguridad encontrados.

5. ALCANCE Y DELIMITACIÓN DEL PROYECTO

En el desarrollo del proyecto se va a implementar un servidor bajo entorno Linux en distribución Ubuntu, y se va a instalar la aplicación SNORT para la generación de reportes de las alertas de eventos de seguridad encontrados, se crearan unas reglas para monitorear el acceso a ciertas paginas no permitidas y se monitoreara el ping a diferentes servidores de la organización, además trabajara en compañía de un servidor de red también sobre Ubuntu server el cual tiene instalado el Proxy Squid y el Firewall Iptables.

Solo se realizara el trabajo de análisis de las alertas de los eventos de seguridad encontrados, pero por el momento por operatividad y costos no se trabajara en la eliminación de las amenazas que este arroje.

6. MARCO REFENCIAL

6.1. MARCO TEÓRICO

- LINUX: Es un sistema operativo el cual su código es libre y abierto para ser utilizado, modificado y mejorado según convenga por varias personas o comunidades, que contribuyen a este componente central que se diversifica en muchos productos los cuales podemos llamar distribuciones

Estas distribuciones ofrecen soluciones para todas las necesidades tanto personales como empresariales, desde sistemas operativos para servidores de redes, bases de datos, aplicaciones, auditorias y seguridad, hasta sistemas operativos para teléfonos móviles inteligentes como lo es Android.

- UBUNTU: Ubuntu es un sistema operativo bajo entorno Linux de código abierto, que permite la implementación de herramientas de seguridad y monitoreo de información para garantizar y salvaguardar la información de redes y elementos informáticos en las organizaciones.

Ubuntu es una derivación del sistema operativo debían, pero mejorado, con menos falencias y más fácil e intuitivo para el usuario, La primera versión de Ubuntu se lanzó el 20 de octubre de 2004, y en la actualidad cubre aproximadamente el 50 % del mercado dentro de las distribuciones Linux.

- IDS/IPS:

Definición: Es un sistema de detección y prevención de intrusos que de acuerdo a parámetros de comportamiento de la red, rechaza o permite el tráfico de datos de información para prevenir posibles amenazas o ataques a los cuales la organización se encuentra expuesta, también muestra las estadísticas y realiza informes correspondientes en cuanto a los reportes de las alertas de los eventos de seguridad generados y accesos no autorizados, permitiendo así a los administradores del sistema de información realizar la toma de decisiones adecuada para salvaguardar los activos de información de la organización.

Función de un IDS: Determinar los riesgo los cuales se encuentra expuesta nuestra red mediante parámetro de comportamiento, gráfico y estadístico, para que el administrador del sistema de información tome las medidas necesarias para prevenir las amenazas existentes

En el modo de prevención de intrusos analiza la información de la red y por medio de su base de datos de amenazas actualizada, puede actuar rechazando las conexiones poco seguras para evitar diferentes tipos de ataques que pueden afectar la disponibilidad, integridad, o confidencialidad de la información.

Tipos:
- ✓ HIDS: Trabaja únicamente en el Equipo que se instala.
- ✓ NIDS: ES orientado a redes, opera modo Snifer.
- ✓ DIDS: Sistema de detección de intrusos de red donde distribuye los sensores en diferentes nodos o equipos

Características:
- ✓ Debe ser autónomo.
- ✓ Tolerancia a fallos.
- ✓ Monitorearse así mismo.
- ✓ No ser una carga extra para el sistema.
- ✓ Determinar cambios de comportamiento.
- ✓ Adaptabilidad.
- ✓ Ser confiable.

Arquitectura de un IDS
La arquitectura de un IDS, está formada por:
- ✓ Recolección de datos.
- ✓ Reglas para detectar patrones anormales de seguridad en el sistema.
- ✓ Filtros para comparar los datos interceptados de la red o de Logs con los patrones que contienen las reglas.
- ✓ Detectores de eventos anormales en el tráfico de red.
- ✓ Generador de informes y alarmas.

- SNORT: Es uno de los sistemas de detección y prevención de intrusos más importantes y populares del momento, es software libre y puede almacenar bitácoras en Mysql, proviene de un programa basado en Linux creado en 1998 llamado APE, el cual era muy limitado y básico, de ahí partió la base para el desarrollo de este sistema de prevención y detección de intrusos.

Snort es un IDS/IPS, Rápido, Flexible, Confiable y potente, posee una gran cantidad de reglas para Backdoors, Ataques de denegación de servicio, Ataques Web, Nmap, que se actualizan mediante internet

- BASE: (Basic Analysis and Security Engine) Utilidad web basada en PHP cuyo objetivo es realizar una gestión fácil, amigable, segura y cómoda, de las bases de datos que generan diferentes tipos de Sistemas de prevención de intrusos, Cortafuegos, y sistemas de monitoreo de red.

6.2. MARCO CONCEPTUAL

- ACCESO NO AUTORIZADO: Consiste en ingresas si el debido permiso, en contra de la voluntad del propietario, administrador, o encargado a un sistema de información, mediante técnicas para encontrar, descifrar o vulnerar contraseñas o sistemas de seguridad.
- ACID: Sistema de detección de intrusos basado en plataformas Linux
- APACHE: Servidor web bajo plataformas Linux
- ATAQUES INFORMÁTICOS: Su objetivo primordial es afectar un sistema de información, mediante la vulneración de la confidencialidad, integridad y disponibilidad de los datos.
- BITÁCORA: Permite llevar registro de acciones y procedimientos
- CONFIDENCIALIDAD: Cualidad de la información que permite que solo sea vista por el personal autorizado.
- DATOS: parte mínima de la información
- DIDS: Sistema de detección de intrusos distribuido
- DISPONIBILIDAD: Cualidad de la información que sea accesible en el momento que se necesite
- DOMINIO DE COLISIÓN: Segmento físico presente en una red de computadores donde las tramas interfieren unas con otras.
- FIREWALL: Es un muro virtual que protege a los sistemas de información de acceso no autorizado.
- GNU: Es un proyecto diseñado en 1983, con el objetivo de realizar un sistema operativo libre y abierto.
- HIDS: Sistema de detección de intrusos basado en host
- IDS: Sistema de detección de intrusos
- INFORMACIÓN: Conjunto de datos procesados
- INTEGRIDAD: Cualidad de la información de mantener los datos sin cambios no autorizados
- IPS: Sistema de prevención de intrusos
- LOGS: son registros o bitácoras que almacenan datos de registro de un programa, Base de datos o sistema.
- MYSQL: Es uno de los sistemas de gestión de base de datos más populares y eficientes en el mercado, desarrollado por Oracle
- NIDS: Sistema de detección de intrusos en red
- NMAP: Aplicación que permite el escaneo de puertos
- PHP: Lenguaje de programación para desarrollo web
- PUERTOS: Es una interfaz que permite la comunicación de aplicaciones a través de la red
- SNIFFER: Detecta cada paquete que viaja por una red para poder ser analizado.
- SOFTWARE LIBRE: Es un software que puede ser utilizado por cualquier persona la cual puede utilizarlo, estudiarlo o editarlo.

- VULNERABILIDADES: Una debilidad o falencia en un sistema de información.
- WEB: Información que se encuentra en una red de internet mediante diferentes protocolos

6.3. ESTADO DE ARTE

Los servidores IDS/IPS han evolucionado a un ritmo lento, pero han presentado mejoras indispensables para generar alertas de eventos de seguridad, entre estas mejoras están en que han añadido servicios de reputación, estos servicios agrupan información acerca de dominios, direcciones IP, protocolos, ubicaciones físicas y otros aspectos de la actividad de la red, en cuanto a sus comportamientos en la red.

Ahora los IDS/IPS, cuentan con análisis de trafico encriptado, el cual su funcionamiento es similar al de un proxy, debido a su rendimiento para trabajar trafico encriptado se recomienda un IDS de host, puesto que el IDS de red puede generar retrasos en la información

- IDS/IPS Para entornos virtuales: Por medio de un gestor de máquina virtual se controla la actividad de red entre una única y diversas instancias, algunos gestores utilizan su propia tecnología de detención mientras que con otros son trasladados a los sistemas de control externos.

- IDS/IPS Wireles: Estos IPS/IDS son los más actuales en el Mercado, permiten detectar conexiones no autorizadas y ataques de los mismos clientes wireles desde la red, también permite gestionar la seguridad en la conexión de dispositivos móviles como Tablets o Smart Phones, lo cual es muy importante debido al auge que estos dispositivos tienen en la actualidad

- IDS/IPS Reconocidos en el mercado:

SURICATA

Es un motor cuyo objetivo es la detección de diferentes amenazas de red, confiable, rápido y robusto, es de licencia GNU.

Suricata es capaz de detectar intrusos en tiempo real, realiza prevenciones de intrusiones en línea, supervisión de seguridad de red y procesamiento offline de PCAP, esta herramienta inspecciona el tráfico de red utilizando una potente y extensa normativa, ofrece un potente soporte de secuencias de comandos LUA para la detección de las amenazas más complejas.

CISCO CATALYST 6500 SERIES

El Cisco IDSM-2 con el software Cisco IPS Sensor v6.0 ayuda a los usuarios a detener más amenazas con mayor confianza, mediante el uso de las siguientes herramientas:

- ✓ Identificación de amenazas multivectoras: una inspección detallada del tráfico de la capa del 2 a la 7 protege a la red de violaciones de políticas, explotaciones de vulnerabilidades y actividad sospechosa en la red.
- ✓ Tecnologías precisas de prevención: cuenta con una tecnología que Cisco califica como innovadora, la cual se base en la calificación de riesgo
- ✓ Meta Event Generator proporcionan la confiabilidad suficiente para tomar acciones preventivas pertinentes con un campo más amplio de amenazas sin el riesgo de perder tráfico legítimo.

6.4. MARCO LEGAL

Este trabajo se rige bajo la ley 1273 de 2009, Ley de delitos informáticos en Colombia.

Capítulo 1 De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

- Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no, tendrá una pena de prisión entre 4 a 8 años y multas entre 100 a 1000 SMLMV
- Articulo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes del mismo, tendrá una pena de prisión entre 3 a 6 años.
- Articulo 269G: Suplantación de sitios web para capturar datos personales: El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, tendrá una pena de prisión entre 4 a 8 años y multas entre 100 a 1000 SMLMV

7. DISEÑO METODOLÓGICO

7.1. TIPO DE INVESTIGACIÓN

Investigación aplicada: Consiste en poner en práctica los conocimientos adquiridos con el objetivo de dar solución a diferentes problemas en escenarios reales.

7.2. MÉTODOS DE INVESTIGACIÓN

El método de investigación que se utilizó para el desarrollo del proyecto fue el de metodología basada en proyectos, y comprende las siguientes fases:

7.2.1. Fases:

- Inicio:

En esta fase Identificamos los requerimientos como servidor y demás materiales para la instalación del IDS/IPS, redactamos la propuesta específica del proyecto, determinamos objetivos, alcance y como se va llevar a cabo el proyecto, se evalúan los riesgos y se hace un estimación de tiempos y costos.

- Planificación:

En esta fase se planifican todas las actividades importantes para el desarrollo de proyecto, se definen como queremos alcanzar a cumplir con los objetivos propuestos por medio de cronogramas de trabajo, estableciendo un presupuesto claro y real.

- Ejecución:

Ponemos en práctica lo implementando, y lo definido entre la etapa de inicio y planificación para el desarrollo del IDS/IPS para la empresa Transporte TMC.

- Monitoreo y Control:

En esta etapa se lleva a cabo una revisión de los objetivos con el fin de determinar su correcto cumplimiento y en el caso de no ser así tomar los correctivos necesarios.

- Cierre:

Realizamos un informe correspondiente indicando el cumplimiento de los objetivos y realizando las revisiones correspondientes entre lo planeado y ejecutado en el desarrollo del IDS/IPS indicando los resultados obtenidos.

7.3. HIPÓTESIS

Hi

Los Sistemas de detección y prevención de Intrusos, ayudan a proteger y a disminuir los riesgos de seguridad de la información dentro de la empresa transportes TMC S.A.S

Ho

Los Sistemas de detección y prevención de Intrusos, no ayudan a proteger y a disminuir los riesgos de seguridad de la información dentro de la empresa transportes TMC S.A.S

7.4. VARIABLES E INDICADORES

Capacidad que tiene la empresa transportes TMC para proteger la información de los riesgos de seguridad informática

Medidas:

Alto, Medio, Bajo Ninguno

Dimensiones

Políticas de Seguridad en general, Asignación de niveles de permiso, Inversión en dispositivos de seguridad, Sistemas de detección y prevención de intrusos

7.5. UNIVERSO

La Implementación del IDS/iPS en Ubuntu Linux en la empresa Transportes TMC, va a utilizarse en todas las áreas de la empresa transportes TMC sede Villavicencio meta. Debido a que todas las áreas están expuestas a afectaciones de disponibilidad integridad y confidencialidad de la información

7.6. INSTRUMENTOS PARA LA RECOLECCIÓN DE INFORMACIÓN

El instrumento empleado para recolectar información sobre la implementación de un IDS/IPS en Ubntu Linux en la empresa Transportes TMC entrevista directa con la gerencia realizando las siguientes preguntas:

- ¿La empresa Transportes TMC S.A.S ha tenido en el último año ataques que afecten la disponibilidad, confidencialidad e integridad de la Información?
- ¿Para la gerencia de Transportes TMC S.A.S es importante invertir en sistemas de seguridad informática que disminuyan los riesgos de algún tipo de afectación de la información?

- ¿La continuidad del negocio se ha visto afectada por intrusiones no autorizadas a alguno de los diferentes equipos informáticos de la empresa Transportes TMC?

- ¿La gerencia de transportes TMC tiene la conciencia y el conocimiento para determinar el impacto que puede causar un ataque que afecte la disponibilidad, confidencialidad e integridad de la información?

- ¿Está dispuesta la empresa transportes TMC en Financiar los costos para la instalación y configuración de un IDS/IPS Snort bajo entorno Linux?

8. ESQUEMA TEMÁTICO

8.1. LEVANTAMIENTO DE INFORMACIÓN DEL ESTADO ACTUAL DE TECNOLOGÍA Y SEGURIDAD, EVALUANDO LA SEGURIDAD INFORMÁTICA DE LA EMPRESA TRANSPORTES TMC.

8.1.1. Estado actual de la tecnología

Tabla 1. Estado actual de la Tecnología

Componente	Características	Años de uso
Servidor de aplicaciones	Dell T320, procesado Intel Xeon E5 2430, 16G de Ram, Raid 1 de 1Tera, Raid 1 DE 2Teras, Sistema operativo Windows server 2012	4 Años de uso
Servidor de dominio	Dell T110, Procesador Intel Xeon 3Ghz, 8G de Ram, Sistema operativo Windows server 2003	12 años de uso
Servidor Proxy	Computador Janus, Intel Celeron de 3Ghz, 4G Ram, D.D 500G, Sistema operativo Ubuntu Server	2 años de uso
Estaciones de Trabajo	Lenovo G40-70 Procesado Intel Core i5, 4G Ram, Disco duro , sistema operativo Windows 7	4 Años de uso
Switch	Trednet DE Giga 24 puertos de Rack	6 años de uso
Internet	Canal de fibra óptica 24 Megas	7 años de uso
AccesPoint Inalambrico	Ubiquiti Unifi Uap Lr	3 años de uso
Ups	2 Ups 6 Kva	7 años de uso

Fuente: El autor

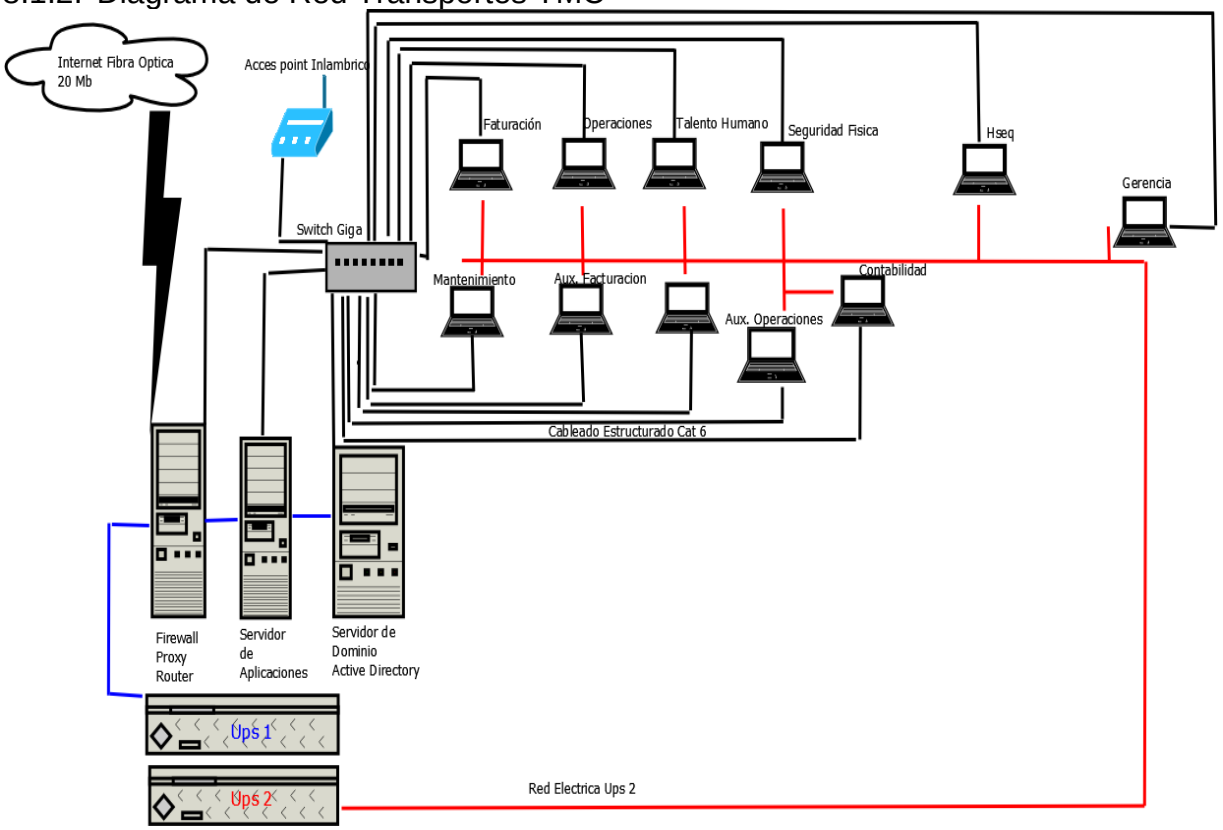
Tabla 2. Elementos de Seguridad De la Empresa

Elemento	Característica	Licencia
Firewall	Iptables en Ubuntu Server, puertos de escritorio remoto, ftp, http abiertos	Libre
Antivirus Servidores	Kaspersky end point security selec, Control de endpoind, antivirus de archivos, web, chat, internet, correo Firewall	1 año, 12 Estaciones
Proxy	Squid, se bloquean paginas no permitidas, entre redes sociales, correos no corporativos y video por streming	Libre
Antivirus Estaciones de Trabajo	Microsoft Security Esentials, antivirus de archivos y trabaja con el firewall de Windows 7	Free con el sistema operativo Windows

Fuente: El autor

.

8.1.2. Diagrama de Red Transportes TMC



Fuente: El autor

8.1.3. Evaluación de la seguridad Transportes TMC

Tabla 3. Evaluación de seguridad de la empresa

Tipo de Activo	**Activo de Información**	**Amenazas**	**Vulnerabilidades**
Datos	Carpeta compartida operaciones Carpeta compartida HSEQ	*Errores de los usuarios *Escapes de información *Alteración accidental de la información	*No hay control de cuentas de usuario para las carpetas *no existen Logs de verificación de las carpetas *la información no está cifrada *no hay Jerarquía de permisos
Aplicaciones	Windows server 2003 Windows server 2012 Ubuntu server Sql 2008 Controlador Principal de dominio Servidor Proxy Windows7 Office 2010 Antivirus Kaspersky end point security Nod 32 Antivirus Syscom 40 Transporte	*Avería de origen físico o lógico *Errores de los usuarios *Difusión de software dañino *Errores de mantenimiento-Actualización *Uso no previsto *Destrucción de información	* No hay políticas ni procedimiento de Mantenimiento preventivo de software *Inexistencia de capacitación a usuarios *Utilización de software ilegal y sin licencia *Ineficiente política restrictiva de utilización manejo e instalación de software *Contraseñas genéricas para el acceso a los sistemas operativos

Tabla 3. (Continuación).

Tipo de Activo	Activo de Información	Amenazas	Vulnerabilidades
Hardware	Servidor de aplicaciones Servidor Proxy Servidor de dominio Pc usuarios Trednet Ubiquiti Unifi	*Fuego *Contaminación mecánica *Errores de mantenimiento-actualización de equipos *Perdida de equipos *Robo	*Instalaciones hechas con materiales inflamables, sin presencia de extintores, *Cuarto de equipos muy poco o nada hermético *No hay políticas de cambios de equipos por vida útil *Inventario ineficiente de equipos *Poca seguridad en el cuarto de equipos
Equipo Auxiliar	Aire acondicionado Ups 6KVA Cableado Estructurado 24 puertos	*Fuego *Contaminación mecánica *Daños por agua *Avería física o lógica	*instalaciones hechas con materiales inflamables, sin presencia de extintores, *Cuarto de equipos muy poco o nada hermético *Aire acondicionado en ubicación inadecuada se tapa y vota agua *Falta de políticas de mantenimiento de aires y ups
Equipos Comunicación	Red Local	*Interceptación de información *Análisis de trafico	*DHCP Activo *No existen procedimiento y políticas en cambios de contraseñas Wifi *SSID Visible

Fuente: El autor

8.2. DETERMINACIÓN DEL SISTEMA DE DETECCIÓN DE INTRUSOS QUE SE VA A IMPLEMENTAR PARA LA EMPRESA TRANSPORTES TMC S.A.S

8.2.1. Evaluación de los Sistemas de Detección de Intrusos

Tabla 4. Evaluación de los sistemas IDS/IPS

Sistema	Snort	Suricata	Catalist 6500 Series
Ventajas	-Licencia GPL -Gratuito -Posee cientos de filtros y reglas -Funciona Como Sniffer -Cumple funciones de firewall -Es uno de los IDS/IPS más utilizados debido a su confiabilidad -Debido a su tiempo en el mercado ofrece gran estabilidad en comparación con sus competidores	-Licencia GNU -Permite ejecutar varios Subprocesos de manera simultanea -permite llevar estadísticas de rendimiento Saca el máximo rendimiento del Hardware -Es un IDS/IPS emergente con nuevas Características en comparación con la competencia	-Soporte Cisco System -Integrado en el chasis del Swith cisco catalist -Viene con Firewall, VPN, VLAN e IPS -En comparación con sus competidores produce pocos falsos positivos
Desventajas	-No indica si un ataque ha sido exitoso o no. -Debido a su base de datos tan robusta posee una gran cantidad de falsos positivos. No analiza trafico cifrado	-Descarga de actualizaciones de forma manual -nivel de detección para nuevos ataques no es eficiente -No posee Interfaz administrativa No analiza trafico cifrado	-Implementación Costosa -Baja escalabilidad -Configuración limitada No analiza trafico cifrado
Facilidad de configuración	Media conocimientos en Linux	Media conocimientos en Linux	Media conocimientos en Cisco
Actualización	Manual	Manual	automática
Tiempo en el mercado	19 años	7 años	15 años
Popularidad en mercado	Alta	Media	Baja
Estabilidad	Alta	Medio - Alto	Alta
Escalabilidad	Alta	Alta	Limitada

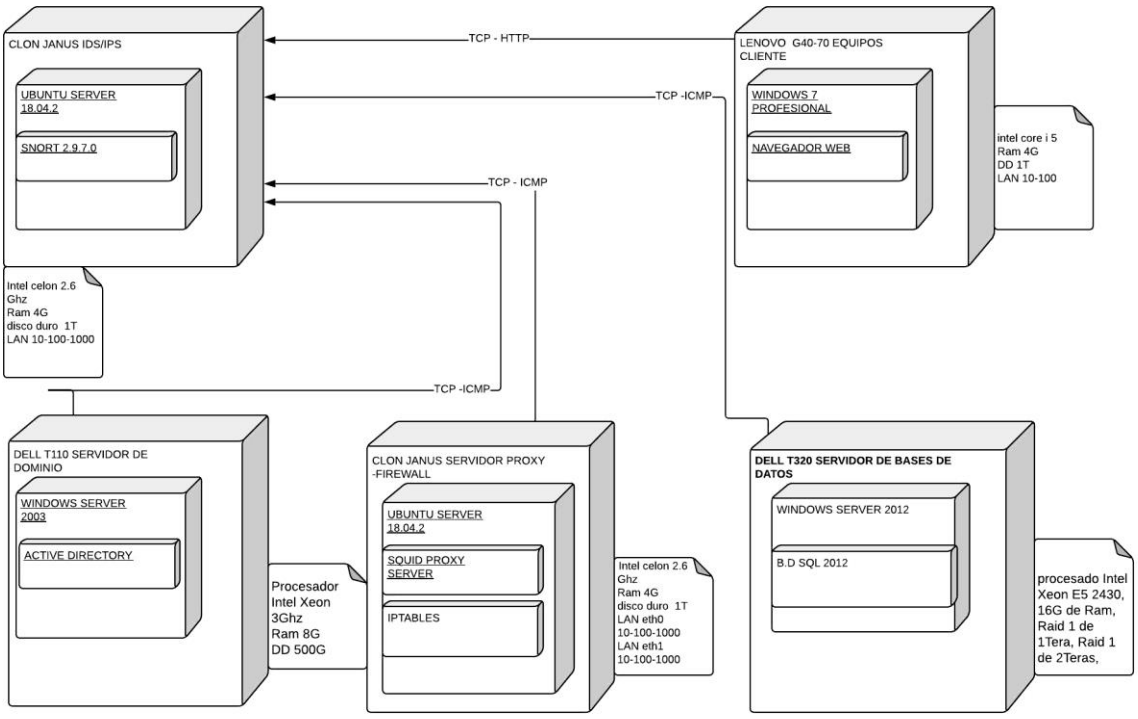
Valor de implementar	Entre $800.000 y 2.000.000	Entre $800.000 y 2.000.000	$10.000.000

Debido a la evaluación realizada de los diferentes sistemas de detección de intrusos más populares, presentes en el mercado, se determina que IDS/IPS que se va a utilizar para la empresa Transportes TMC S.A.S es Snort por las siguientes características:

- Confiabilidad: Es uno de los IDS/IPS Mas confiable del mercado
- Tiempo en el mercado: ES el IDS/IPS que más tiempo tiene en el mercado contando con19 años de evolución y experiencia
- Precio: Es de licencia GNU, por lo tanto solo se asumen los costos del Hardware a implementar
- Posee una gran cantidad de filtros y reglas
- Muchos IDS/IPS Están Basado en Snort
- Existen diferentes manuales para implementación en la red

8.3. PRUEBAS DE CONFIABILIDAD IDS/IPS SNORT.

8.3.1. Diagrama de Implementación



9. PROPONENTES DEL PROYECTO

9.1. PRIMARIOS

Cesar Enrique Silva Garcia Se graduó como tecnólogo de la Fundación Universitaria CIDCA en el año 2005 y luego como Ingeniero de sistemas de la universidad Remington De Medellín en el año 2012

Su experiencia profesional está enfocada a la administración, montaje y soporte de Servidores Bajo entorno Linux y Windows, brindando mediante alianzas soluciones informáticas para cualquier tipo de organización.

9.2. SECUNDARIOS

Juan José Cruz Garzón, Ingeniero de sistemas, Especialista en seguridad informática, Candidato a magister en Seguridad Informática, Candidato a magister en el MBA en Negocios Internacionales, docente ocasional Universidad Nacional Abierta y a Distancia.

10.RECURSOS NECESARIOS PARA EL DESARROLLO

10.1. RECURSOS MATERIALES

- Papelería
- Cpu marca Janus Procesador Intel Celeron 2,2, 4G de Ram, DD 512
- Tarjeta de red Tp Link 1G
- Internet banda ancha
- Patch cord certificado Cat 6

10.2. RECURSOS INSTITUCIONALES

Las oficinas de Transportes TMC S.A.S

10.3. PRESUPUESTO

Tabla 5. Presupuesto

RECURSO	DESCRIPCIÓN	VALOR
Humano	Instalación y configuración de un IDS/IPS con sus respectivos manuales	1.000.000
Papelería	Fotocopias, impresiones otros	30.000
Cpu marca Janus	Procesador Intel Celeron 2,2, 4G de ram DD, 512G	700.000
Tarjeta de red Tp link 1G	Tarjeta de red externa para la LAN.	30.000
Internet banda ancha	Para investigación, descarga y actualización del sistema operativo	30.000
Patch cord certificado Cat 6	Para conexión del servidor IDS/IPS al Switch	20.000
TOTAL		**$ 1.810.000**

Fuente: El autor

11. RESULTADOS E IMPACTOS ESPERADOS

Al implementar un IDS/IPS Snort En Ubuntu para la empresa Transportes TMC S.A.S disminuirá los riesgos de intrusiones no autorizadas a las que se encuentran expuestos los datos informáticos, tales como ataques de denegación de servicio, Ramsomware, vulneración a través de Exploits, robo de información, Spoofing entre otros, aumentando o manteniendo la operatividad constante en el área de informática de la organización, reduciendo costos en reparaciones y evitando perdida de dinero por parálisis de actividades o robo bancario que puede causar un gran impacto en las finanzas de la compañía.

12.DIVULGACIÓN

Autorizo la divulgación y publicación del presente trabajo a la universidad Nacional Abierta y a Distancia UNAD el cual puede ser revisado contra plagio y para que sea almacenado en el repositorio de trabajos de grado.

13.CRONOGRAMA DE ACTIVIDADES

NOMBRE DE LA EMPRESA:	TRANSPORTES TMC
RESPONSABLES DE LA IMPLEMENTACION	CESAR ENRIQUE SILVA GARCIA

ACTIVIDAD	RESPONSABLE	SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
		SEMANA				SEMANA				SEMANA				SEMANA			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
SOLICITUD DE MATERIALES	CESAR SILVA																
INSTALACION IDS/IPS SNORT	CESAR SILVA																
ENTREGA DE MANUALES Y DOCUMENTOS	CESAR SILVA																
GRAFICA VULNERABILIDADES ENCONTRADAS	CESAR SILVA																

14.CONCLUSIONES

1. De acuerdo a el análisis de los diferentes IDS/IPS en el mercado, podemos concluir que Snort es confiable, seguro y se ajusta a las necesidades de la empresa Transportes TMC S.A.S

2. Las empresas se encuentran bajo el constante riesgo de las amenazas existentes en constante crecimiento, como consecuencia deben estar un paso adelante buscando herramientas de detección y prevención de intrusiones que puedan garantizar la integridad confidencialidad y disponibilidad de la información.

3. Linux en sus diferentes distribuciones, nos ofrece herramientas por un bajo costo, que nos permiten aumentar y mantener la seguridad en nuestras organizaciones, estando a la vanguardia de nuevas tecnologías y a los retos en cuanto a vulnerabilidades y amenazas que se presentan.

15.RECOMENDACIONES

1. Tomar en cuenta las observaciones dadas por departamento I.T sobre las posibles detecciones de intrusos que arroje el programa Snort, para tomar las correspondientes acciones a las que haya lugar.

2. Se recomienda realizar capacitaciones periódicas al personal sobre los posibles ataques de ingeniería sociales los cuales se encuentra expuesta la organización, que por más medidas de seguridad que se implementen el usuario siempre será el primer guardián de la seguridad y la información.

3. Establecer políticas de seguridad de la información que sean coherentes con la implementación del sistema de detección y prevención de intrusos.

16.BIBLIOGRAFÍA

GRAFTON, Pilar y NAVIA, Luisa. Cómo el docente puede obtener la información que necesita para su labor. Primera Edición. La Habana, Editorial Pueblo y Educación. 1992, 73 p.

WEBGRAFIA

Breve introducción a los sistemas IDS y Snort. [En línea], Agosto 19 de 2003, [Revisado: Octubre 2017]. Disponible en internet: http://www.maestrosdelweb.com/snort/

Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Module. [En línea], [Revisado: 10 de septiembre de 2017]. Disponible en Internet: http://www.cisco.com/c/en/us/products/interfaces-modules/catalyst-6500-series

Metodología de la investigación documental. [En línea]. [Revisado el 10 de septiembre de 2017]. Disponible en Internet: https://www.ecured.cu/Metodolog%C3%ADa_de_la_investigaci%C3%B3n_documental

Norma Técnica Colombia, Biblioteca virtual Unad. [En línea]. [Revisado el 12 de septiembre de 2017]. Disponible en Internet: http://campus14.unad.edu.co/ecbti09/pluginfile.php/4313/mod_page/content/6/NTC1486.pdf

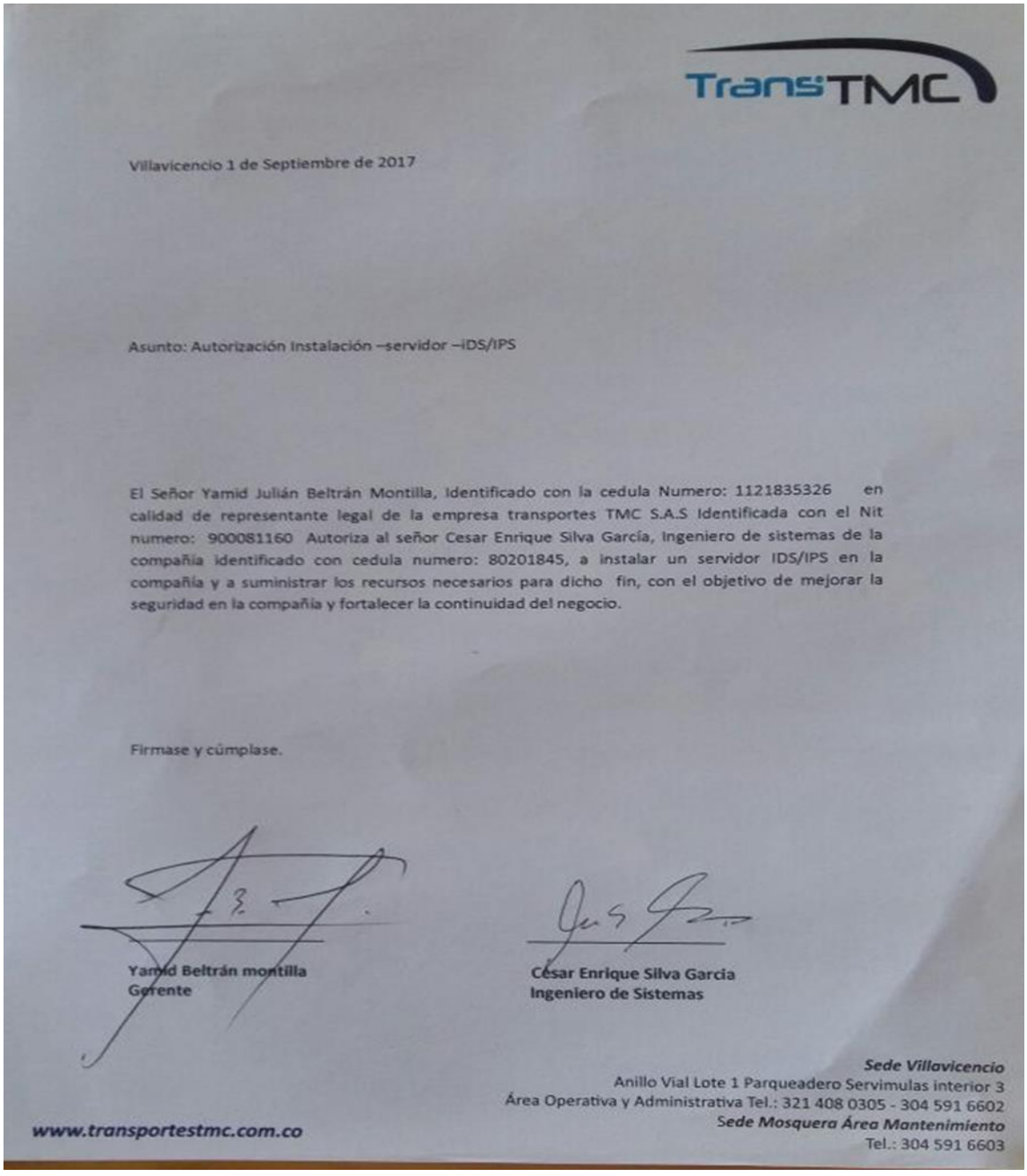
SCARFONE Karen, Tecnologías IPS/IDS: cambios e innovaciones. [En línea]. [Revisado el 12 de septiembre de 2017].Disponible en Internet: http://searchdatacenter.techtarget.com/es/consejo/Tecnologias-IPS-IDS-cambios-e-innovaciones

Sistemas IDS/IPS. [En línea]. [Revisado el 12 de septiembre de 2017] Disponible en Internet: http://maestroseguridades.es.tl/IPS-_-IDS.htm

Suricata. [En línea]. [Revisado el 12 de septiembre de 2017]. Disponible en Internet: https://suricata-ids.org/

ANEXOS

ANEXO A. Carta de aprobación instalación IDS/IPS Transportes TMC S.A.S



Trans TMC

Villavicencio 1 de Septiembre de 2017

Asunto: Autorización Instalación –servidor –iDS/IPS

El Señor Yamid Julián Beltrán Montilla, Identificado con la cedula Numero: 1121835326 en calidad de representante legal de la empresa transportes TMC S.A.S Identificada con el Nit numero: 900081160 Autoriza al señor Cesar Enrique Silva García, Ingeniero de sistemas de la compañía identificado con cedula numero: 80201845, a instalar un servidor IDS/IPS en la compañía y a suministrar los recursos necesarios para dicho fin, con el objetivo de mejorar la seguridad en la compañía y fortalecer la continuidad del negocio.

Firmase y cúmplase.

Yamid Beltrán montilla
Gerente

César Enrique Silva García
Ingeniero de Sistemas

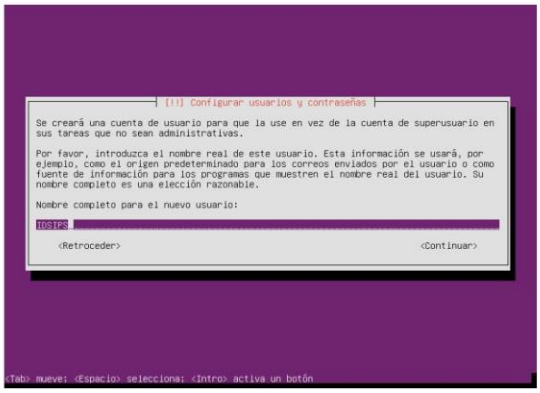
Sede Villavicencio
Anillo Vial Lote 1 Parqueadero Servimulas interior 3
Área Operativa y Administrativa Tel.: 321 408 0305 - 304 591 6602
Sede Mosquera Área Mantenimiento
Tel.: 304 591 6603

www.transportestmc.com.co

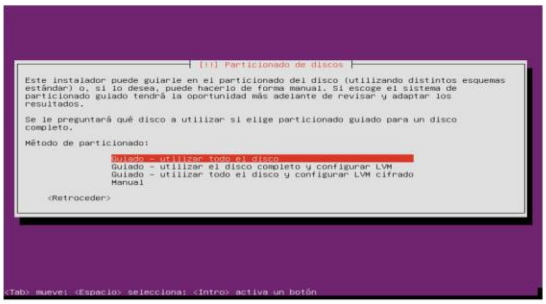
MANUAL DE FUNCIONAMIENTO IDS/IPS SNORT EN UBUNTU LINUX

Instalación Ubuntu Linux

Colocamos el nombre de usuarios y la contraseña de nuestro servidor.

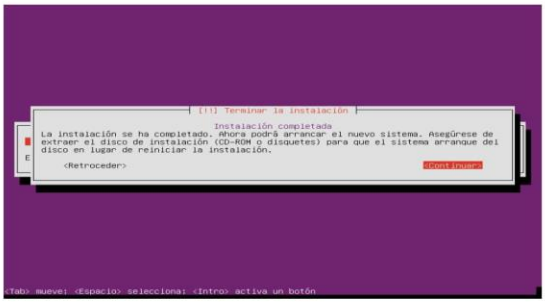


Método de particionado utilizado, Guiado – Utilizar Todo el Disco



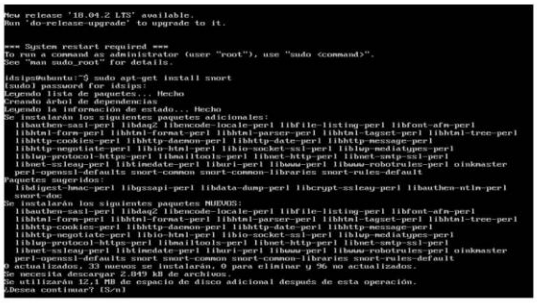
Instalamos el cargador de arranque GRUB en el disco duro

Al terminar la instalación solo damos click en continuar



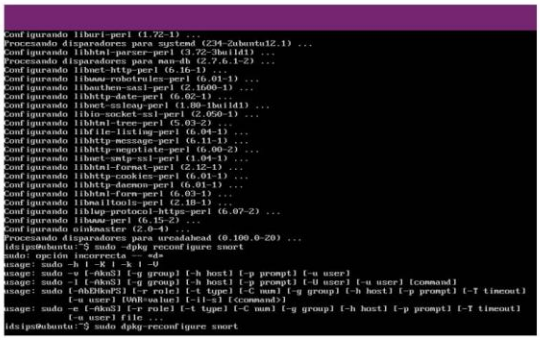
Instalación de Snort

Con el comando sudo apt-get install snort

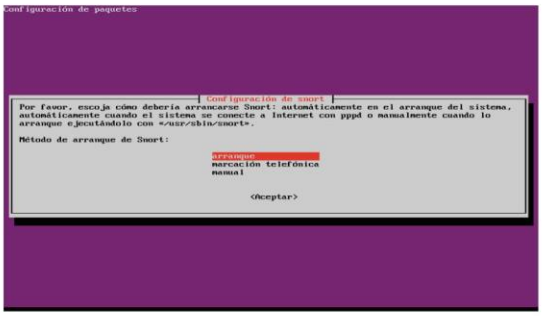


Configuración de snort

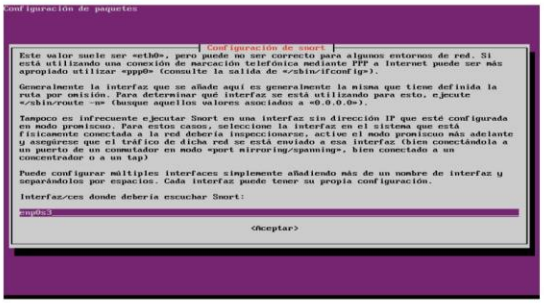
Utilizamos el comando sudo dpk-reconfigure snort



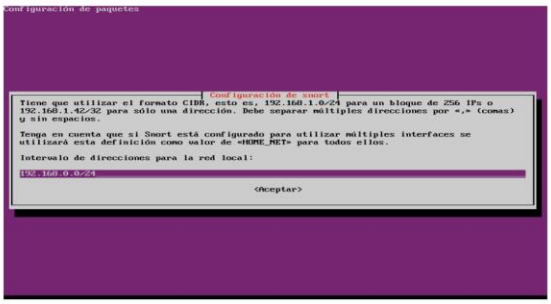
El inicio de snort lo dejamos por medio del arranque del S.O



Damos el nombre de la interfaz de red la cual escuchara todo el tráfico de la red, enp0s3

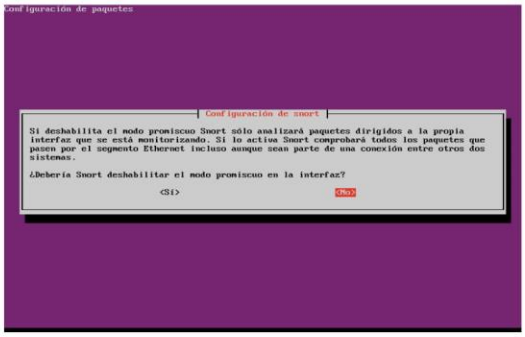


Luego configuramos el formato CIDR, indicando que el intervalo de direcciones a analizar es el segmento de IP clase C, 192.168.0.0/24

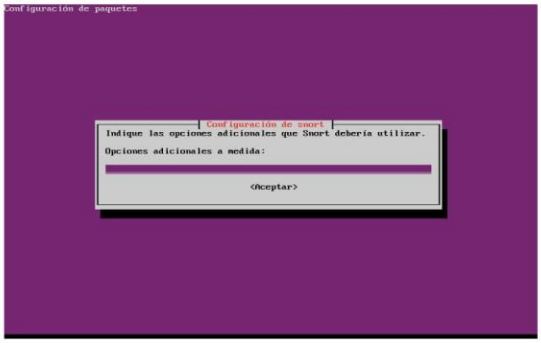


Dejamos activo el modo promiscuo para escanear

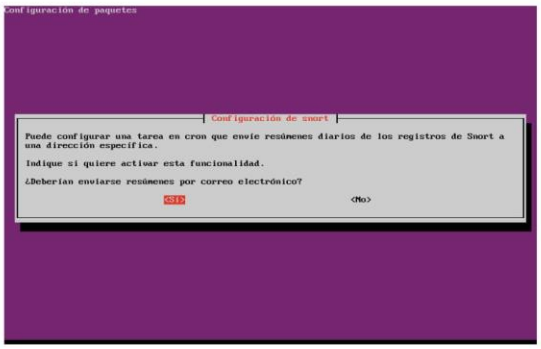
Toda la red

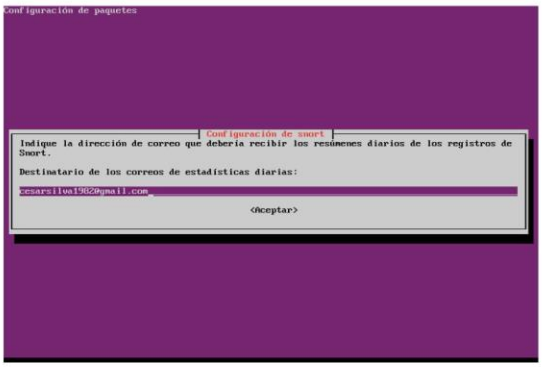


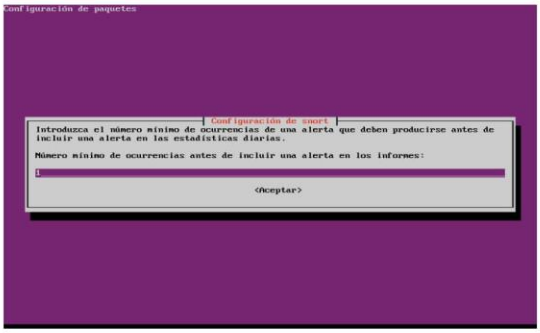
No configuramos opciones adicionales



Configuramos el envió de registros automáticamente







Ahora creamos el archivo de alertas personalizado llamado sites.rules, con sudo nano /etc/snort/rules/sites.rules

Configuramos las reglas para que nos informe quienes están accediendo a páginas web no permitidas, si tenemos escaneo de puertos y también si se está realizando ping a alguno de los equipos

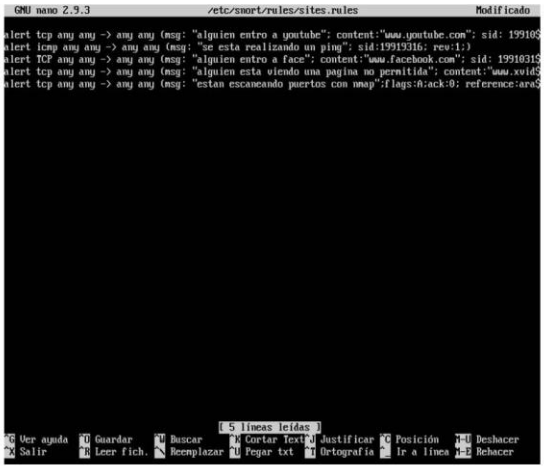
Reglas:

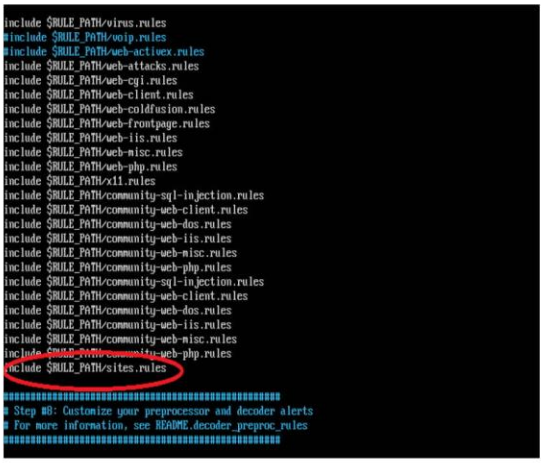
- alert tcp any any -> any any (msg: “alguien entro a youtube”; content: “www.youtube.com”; sid: 19910314; rev:1;
- alert tcp any any -> any any (msg: “alguien entro a youtube”; content: “www.facebook.com”; sid: 19910315; rev:1;
- alert tcp any any -> any any (msg: “alguien entro a youtube”; content: “www.xvideos.com”; sid: 19910317; rev:1;
- alert icmp any any -> any any (msg: “se esta realizando un ping”; sid: 19910316; rev:1;

Luego configuramos el archivo snort.conf con el comando: sudo nano /etc/snort/snort.conf

Luego agregamos la regla en el paso número 7 de personalización

Include $RULE_PATCH/sites.rules

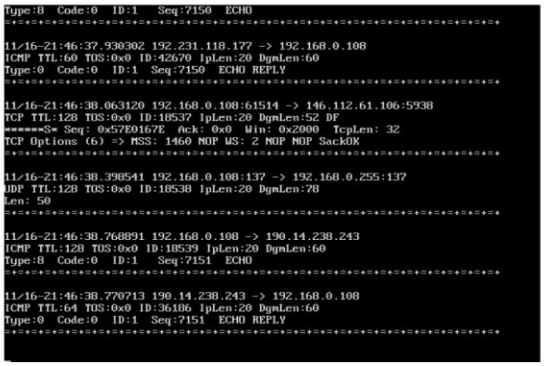




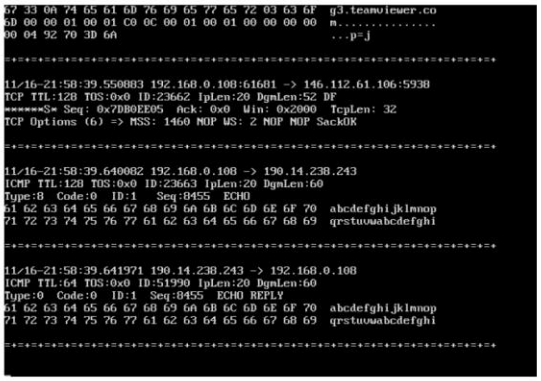
Comandos de uso:

Todos los comandos en el sistema se deben ejecutar como administrador, por lo tanto se debe anteponer a cada comando la instrucción sudo.

- Snort –v: Este comando convierte nuestro IDS/IPS en modo snifer, es decir monitorea todos los paquetes que circulan por la red, mostrando direcciones IP, cabeceras de tipo TCP,UDP E ICMP, de la empresa Transportes TMC



- Snort –d: Muestra información detallada del tráfico TCP, UDP e ICMP.

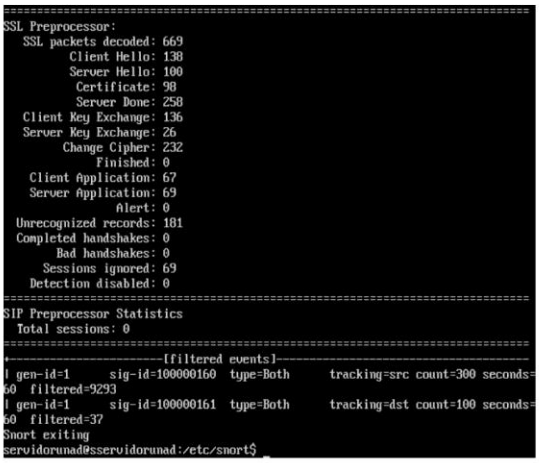


- -c: Espeifica el archivo de configuración snort.conf
- -i: Con este comando especificamos la interfaz de red LAN donde obtenemos los datos
- not host: Este comando permite rechazar o ignorar el tráfico procedente de una dirección IP
- Src net: permite rechazar o ignorar el tráfico de un segmento de red.
- Src port: Rechaza o ignora el tráfico que tenga el puerto indicado con la IP correspondiente.

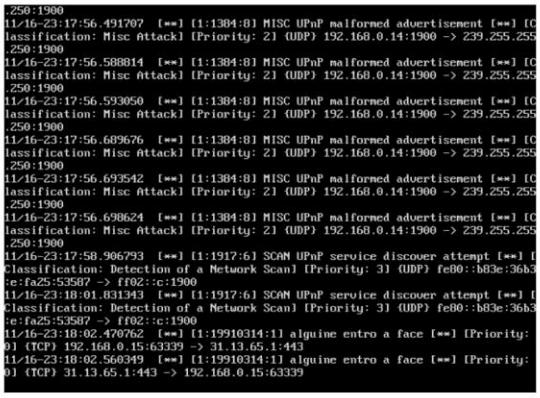
- /etc/init.d/snort start: Iniciamos el servicio Snort

- /etc/init.d/snort stop: Con este comando detenemos el servicio Snort.

- Con las teclas ctrl + c Paramos la actividad de análisis del IDS y nos da un reporte.

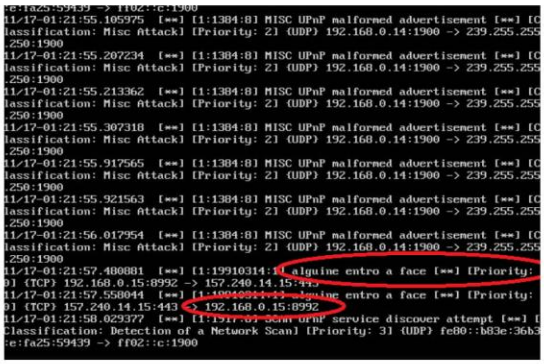


- Snort –A console –c snort.conf –I enp0s3: Con este comando iniciamos en modo detección y
- prevención de intrusos de Snort

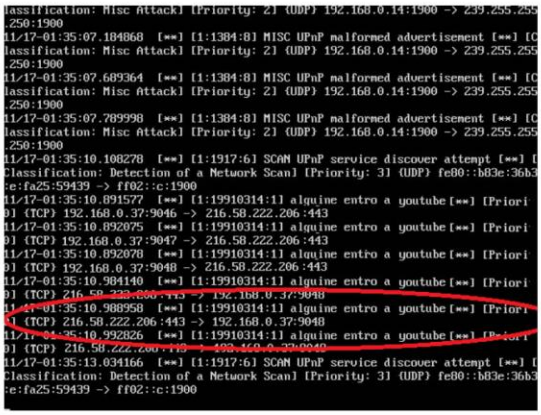


Pruebas a las reglas definidas

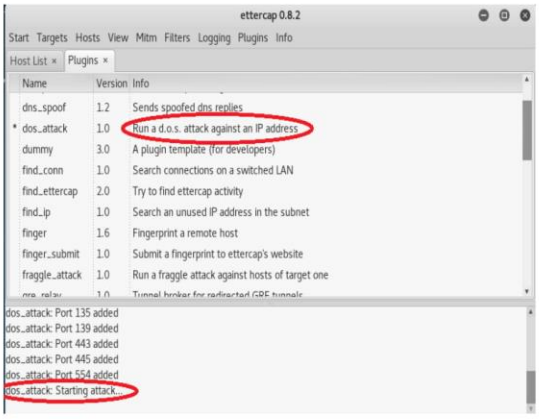
Creamos una regla que nos informe el momento en el que alguien de la red ingresa a una página web no permitida, en este caso lo haremos con Facebook.com - Youtube.com, nuestro IDS/IPS ha detectado este acceso no autorizado y no lo ha informado, proveniente de la ip 192.168.0.15.



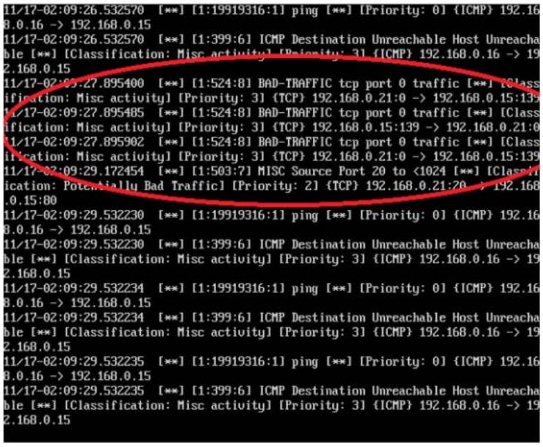
Tambien podemos ver que desde la direccion ip 192.168.0.37 accedieron al pagina Youtube.com.



Ahora vamos a simular un ataque por medio de una aplicaion presente en Kali Linux, Ettercap, realizamos un ataque DDOS, para ello utilizaremos la IP 192.168.0.21 para direccionar todos los paquetes de la red a el equipo victima, cuya direccion IP es 192.168.0.15



Luego podemos ver que nuestro IDS/IPS ha detectado el ataque correspondiente desde la IP 192.168.0.21 a la ip 192.168.0.15, y ha bloquedo la IP del atacante



ANEXO C. Formato Alertas de Eventos de Seguridad Encontrados, Transportes TMC S.A.S

FORMATO ALERTA DE EVENTOS DE SEGURIDAD ENCONTRADOS AÑO 2017						
Semana	ingresos Web no autorizados	Ataques DDos	Escaneo de puertos	alertas TCP	Alertas UDP	otro
1- (10 de Noviembre)	120		10	2505	4325	2008
2- (17 de Noviembre)	242		24	3330	3456	3476
3- (24 de Noviembre)						
4- (1 de Diciembre)						
5-(8 de Diciembre)						
6- (15 de Diciembre)						
7- (22 de Diciembre)						
8- (29 de Diciembre)						

ANEXO D. Grafica Alertas de Eventos de Seguridad Encontrados, Transportes TMC S.A.S