IMPLEMENTACION DE UN SISTEMA DE DETECCION DE INTRUSOS PARA LA RED LOCAL DE LA FERRETERIA CORINTIOS EN SANTA MARTA.

HUGO ALBERTO PAYARES BECERRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

SANTA MARTA – MAGDALENA

2016

IMPLEMENTACION DE UN SISTEMA DE DETECCION DE INTRUSOS PARA LA RED LOCAL DE LA FERRETERIA CORINTIOS EN SANTA MARTA.

HUGO ALBERTO PAYARES BECERRA

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

Director de Proyecto

ING. YINA ALEXANDRA GONZALEZ SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

SANTA MARTA – MAGDALENA

2017

Nota de aceptación:

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Santa Marta, 20 de Noviembre del 2017

DEDICATORIA

Al creador de todas las cosas, el que me ha dado la fortaleza y humildad que de mi corazón puede emanar, dedico primeramente mi tesis de grado a yahweh.

También dedico mi proyecto de tesis a mi esposa que durante el proceso de estudio de la especialización siempre ha estado a mi lado y brindándome su apoyo y comprensión.

A mis Hijos que son la inspiración de seguir adelante en este proyecto de especialista.

A mi madre que ha sabido formarme con buenos sentimientos, hábitos y valores, los cuales me ayudan para seguir adelante y afrontarlos de la mejor forma.

AGRADECIMIENTOS

Doy Gracias a nuestro Padre el Todopoderoso por guardarme durante el proceso de mi tesis y darme las fuerzas necesarias para cumplir con los objetivos planteados en mi proyecto.

También a la ferretería Corintios por facilitarme los medios y recursos, y brindarme el apoyo para el desarrollo de esta investigación como futuro especialista en seguridad informática de la universidad Nacional Abierta y A Distancia de santa marta. Con los lineamientos del proyecto para que se cumplan bajo los parámetros necesarios.

Un agradecimiento por todo el interés mostrado por mi proyecto y todas las sugerencias de mi tutora la ingeniera Yina Alexandra González Sanabria, quien deposito toda su confianza y exploto todas mi fortalezas para llegar a mi propósito en mi trabajo.

TABLA DE CONTENIDO

Pag.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

SNORT: Es un sistema de detección de intrusos de redes de software de código abierto y licencia a gratis[1].

SMTP: (Protocolo para transferencia simple de correo) es un protocolo d red para el intercambio de mensajes de correo electrónico entre computadores u otros dispositivos[2].

SWITCH: Dispositivo de interconexión de redes informáticas[3].

REGLAS: Firmas o reglas son el corazón del motor de detección de intrusiones del Snort[4].

PHISHING: Técnica de ingeniería social para la suplantación de identidad adquiriendo información de la manera fraudulenta que se comete para generar un delito informático.[5]

IDS: (sistema de detección de intrusiones) programa de detección de acceso no autorizado a un computador o a una red[6].

---

[1] SNORT, ¿Qué es Snort?, Marzo 30, 2016. página web disponible en: https://www.snort.org/faq/what-is-snort

[2] SMTP, (Protocolo simple de transferencia de correo) 26 marzo 2017. Disponible en: https://www.ibm.com/support/knowledgecenter/es/ssw_i5_54/rzair/rzairemcommnd.htm

[3] SWITCH, Conmutador (dispositivo de red). Abril 15 2017. Disponible en: https://es.wikipedia.org/wiki/Conmutador_(dispositivo_de_red)

[4] REGLAS, snort. ¿Qué es una regla de Snort?, 2016. página web disponible en: https://www.snort.org/faq/what-is-a-snort-rule

[5] PHISHING. ¿Qué es Phishing?. Marzo 26 2016.https://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/

[6] MIRA ALFARO, Emilio José. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Proyecto Final de Carrera. Valencia – España. Universidad de Valencia. Facultad de Ingeniería. 2001. 13 p.

LOGS: Archivo de evidencia del comportamiento del sistema de detección de intrusiones generados en sus procesos determinados[7].

TCP: (Tranmission Control Protocol) Protocolo de control de transmisión que es utilizado fundamentalmente en internet[8].

CIBERSEGURIDAD: Conjunto de herramientas que se utilizan para salvaguardar y proteger los activos de una organización y los usuarios en su entorno[9].

VIRTUALBOX: Software de virtualización y la instalación de sistemas operativos dentro de un mismo pc[10].

MÁQUINA VIRTUAL: Software que simula una computadora y correr programas en ella como si fuera real[11].

WINPCAP: Herramienta que realiza la conexión para acceder entre la capa de red en un entorno de Windows[12].

STRAWBERRY PERL: Lenguaje de programación para la plataforma de Windows que contiene un compilador MinGW C/C++.[13]

---

[7] LOGS. Registro de Errores (Error Log). 25 mayo 2017. Disponible en:https://httpd.apache.org/docs/2.0/es/logs.html

[8] TCP. qué significa. 25 MAYO 2017. Disponible en:TCP IP https://definicion.de/tcp-ip/

[9] CIBERSEGURIDAD. Conpes 3701. Capacidad para minimizar el nivel de riesgo, 25 mayo 2017. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-6120.html

[10] VIRTUALBOX. Welcome to VirtualBox.org. 25 mayo 2017. Disponible en: https://www.virtualbox.org/

[11] MÁQUINA VIRTUAL. 25 de mayo 2017 Disponible en:https://es.wikipedia.org/wiki/M%C3%A1quina_virtual.

[12] WINPCAP. ¿Qué es WinPcap?. 25 de mayo 2017. Disponible en: https://www.winpcap.org/docs/docs_412/html/main.html.

[13] STRAWBERRY PERL. Entorno perl. Mayo 25 2017.Disponible en: http://strawberryperl.com/.

MYSQL DATABASE: Código abierto de sistemas de gestión de base de datos relacional.[14]

PHP: Lenguaje de programación de scripting del lado del servidor con el solo propósito para el desarrollo web[15].

BARNYARD2: Interprete de código abierto para los archivos saliente del Snort[16].

DOTNETFX40: Es un componente para la plataforma Net de Microsoft[17].

[14] MYSQL DATABASE. ¿Qué es MySQL? . 25 de mayo 2017.https://www.w3schools.com/php/php_mysql_intro.asp

[15] PHP. ¿Qué es PHP?. Ayo 25 2017. Disponible en: https://www.w3schools.com/php/php_cookies.asp

[16] BARNYARD2. Using Barnyard2 in Snort. Mayo 25 2017. Disponible en: https://www.honorsociety.org/articles/using-barnyard2-snort

[17] DOTNETFX40. Microsoft .NET Framework 4. Mayo 25 2017. Disponible en: https://www.microsoft.com/es-co/download/details.aspx?id=3324

INTRODUCCION

Los desafíos que se contemplan a medida que se da el crecimiento de la tecnología y la información de datos en la red, crecen ante la cantidad de intentos de accesos no autorizados a la información que existe en Internet y que han crecido durante estos últimos años.

La dirección de la Ferretería Corintio, normalmente por motivos de costo ha migrado información valiosa en la nube de internet y también almacenándola en su servidor principal; sin ningún control que esté contrarrestando el análisis de cualquier intruso que visita su red porque no hay controles en la seguridad que conlleva al buen manejo de sus activos y el comportamiento adecuado de los trabajadores por el mal manejo de la información. Esto genera un impacto dentro y fuera de la ferretería Corintios porque se están abriendo puertas para permitir las conexiones entrantes de todos en particular llámese clientes, proveedores, facturas por cancelar y un control en su cartera financiera.

La falta de presupuesto para el área de sistemas y tecnología en la empresa muestra un deficiente vacío donde muchos de los atacantes están al acecho de que cualquier red este libre para poder tomar la información y hasta apoderarse de su red LAN. Esto conlleva a una gran vulnerabilidad que no solo afecta a sistemas tradicionales seguros, sino que afectan incluso a sistemas de seguridad: cortafuegos y sistemas de detección de intrusos o IDS (Intrusion Detection Systems).

Al pasar el tiempo las redes han presentado un crecimiento acelerado, causando mayor preparación con la verificación del tráfico de las redes y el mejoramiento de las buenas prácticas para el control y seguridad sobre los ataques que se van generando durante el tiempo, no ha sido hasta hace poco tiempo que las herramientas para producir análisis sofisticados a redes han llegado a estar disponibles para las masas.

1 PLANTEAMIENTO DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La Ferretería Corintio de la ciudad de Santa Marta es posible que se están presentando ataques de terceros con el propósito de obtener la información sobre la base de datos de sus clientes y los procesos de facturación que se llevan a medida que transcurre el tiempo en su red local.

A medida que las comunicaciones se globalizan, el incremento en la utilización de redes, ya sean estas Intranet o Internet, hacen que los activos informáticos se vean cada vez más propensos a ataques de agentes por medio de la red.

Es bastante patente la necesidad de un Sistemas de Detección de Intrusos en los sistemas, los cuales se basan en la vulnerabilidad de los sistemas operativos para incrementar su infección.

La cantidad de accesos no autorizados a la información que existe en la Internet ha crecido durante los últimos años de una manera significativa, comprometiendo la estabilidad económica, social tanto a nivel empresarial como a nivel doméstico.

En Colombia, las instituciones de seguridad se están vinculando a la Estrategia TI para aumentar la capacidad del Estado de enfrentar las amenazas informáticas, pues en el momento presenta grandes debilidades, pese a que existen iniciativas gubernamentales, privadas y de la sociedad civil que buscan contrarrestar sus efectos.

Los organismos estatales es muy preocupante la vulnerabilidad en cuanto a ciberseguridad se refiere, más aún cuando en estas instituciones se concentra la mayoría de los controles de los sistemas de información del país. Las empresas manejan información comercial sobre sus clientes, empleados, proveedores y terceros de ahí la necesidad de implementar soluciones y procesos que aseguren su información, tanto de amenazas externas como de internas.

La ferretería Corintio está expuesto como la gran mayoría de las entidades privadas a actividades maliciosas y ataques cibernéticos como son: amenazas, phishing,

código malicioso, zombies de spam, computadoras infectadas por bots, orígenes de ataques a redes, etc

Los ataques cibernéticos a que está expuesto la ferretería Corintio pueden ser de dos tipos:

- Externo: Los ataques son realizados desde cualquier parte del mundo por medio del internet.
- Internos: En este caso los ataques pueden ser realizados directamente en la ferretería Corintio, generados internamente por cualquier empleado.

Para la ferretería Corintio la seguridad es algo primordial en el correcto funcionamiento de sus redes de datos, pues con ella se garantiza la confidencialidad, integridad y disponibilidad de la información. Una violación a su seguridad puede ocasionar severos daños a la integridad, las cuales son de vital importancia en la organización y pueden llegar a afectar datos relevantes para los empleados que están usando los sistemas de información.

La ferretería Corintio actualmente no contempla una política de seguridad de la información, basada en la confidencialidad, integridad y disponibilidad de la información de la compañía. Por esto se plantea la necesidad de realizar un estudio de las ventajas y alcances que tiene un IDS, así como su aceptación con respecto a la infraestructura de la seguridad de la compañía.

1.2 FORMULACION DEL PROBLEMA

¿Cuenta la ferretería Corintio con un Sistema de Detección de Intrusos en su red local que detecte la presencia de intrusos y ayude a disminuir las intrusiones internas y externas que comprometen la seguridad de la información?

2 JUSTIFICACION

La implementación de un sistema de detención de intrusos es una extensión de la seguridad para una organización y que a su vez consiste en detectar actividades inapropiadas o incorrectas desde el exterior e interior de un sistema informático.

El presente proyecto nace a raíz del aumento considerado de ataques informáticos que se producen en internet y del avance tecnológico, y a que en la Ferretería Corintios no se cuenta actualmente con una herramienta de defensa ante los intentos de intrusión desde el interior o exterior de la red.

Este Sistema de Detección de Intrusos IDS, permitirá a la ferretería corintio estar a la vanguardia en la seguridad tecnológica con respecto a ferreterías vecinas de la ciudad, lo cual implicara tener un control del acceso e implementación de las políticas de seguridad para reconocer ataques, mantener un registro y tomar las acciones correctiva necesarias. Además con este sistema se reducirán los gastos administrativos ya que para su implementación solo necesitaremos de un computador sin muchos requerimientos.

La implantación del Sistema de Detección de Intrusos no solo beneficiara a la alta gerencia sino también al personal administrativo y/o al personal encargado del área de sistema; ya que le permitirá administrar y mantener un historial de intentos de intrusiones en la red, además tendrá acceso en tiempo real ante un posible ataque.

La decisión de la elaboración del trabajo de grado con Snort, es que este es un sistema IDS basado en red (NIDS). El cual, tiene como característica analizar y capturar paquetes en busca de alertas, registro y cualquier anomalía que presente la red, con la finalidad de evitar las vulnerabilidades que presente dicha información de la organización. Por esta razón se hace necesario implementar un IDS ya que con el desarrollo de este se pretende utilizar los mecanismos necesarios que justifiquen su validez y ejecución beneficiando el manejo de la información en cuanto a seguridad e integridad de la información y así dar pautas o recomendaciones para implementar un IDS en la Ferretería Corintios, implementando la herramienta de detección de intrusos para la red que permita proteger los activos reales de la información digitalizada.

El impacto que genera el presente proyecto es relevante ya que el tema abordado implica un beneficio para la organización

Así mismo este proyecto es realizado con el fin de integrar y aplicar los conocimientos y competencias aprendidas en el transcurso de la Especialización en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD, de la Zona Caribe, CEAD Santa Marta – Magdalena.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Implementar un Sistema de Detección de Intrusos IDS en la red de datos de la ferretería corintio apoyado en medidas de ciberseguridad para disminuir las intrusiones internas y externas de usuarios que comprometen la seguridad de la información.

3.2 OBJETIVOS ESPECIFICOS

- Conocer el estado de la infraestructura y configuración de la red con que cuenta la ferretería Corintio para el diseño e implementación de un sistema de detección de intrusos IDS.

- Provisionar a la Ferretería Corintios de las herramientas tecnológicas necesarias para Implementar el sistema de detección de intrusos y realizar las pruebas pertinentes para determinar los ataques y problemas de gestión de la seguridad.

- Determinar los controles que deben adoptarse en cuanto a la configuración y administración de la red.

- Elaborar un informe final de los resultados de las pruebas y recomendaciones

4 MARCO DE REFERENCIA

4.1 ANTECENDENTES

Al inicio de la aparición de la red de computadores en el mundo, se dio inicio también la importancia de la detección de intrusiones a nivel mundial. Esto conllevo que personas preparadas para la vulnerabilidad de la red en su momento fuera el ojo del huracán, se hizo muy evidente la necesidad de la creación de un sistema de detección de intrusos para prevenir y mitigar los impactos generados por los ataques que en su momento eran la mayor complicación de las redes. Con el presente ha surgido la aparición de cualquier cantidad de herramientas para la vulnerabilidad de los sistemas de información que están implementados en las organizaciones. A continuación, se enuncian algunos antecedentes que nos muestra sobre los sistemas de detección de intrusos para afrontar el presente proyecto aplicado.

Miranda Alfaro[18] nos presenta un Sistema de detección de intrusos que genera un informe diario de todas las alertas y que lo envíe de manera automática por correo electrónico al administrador de seguridad para que se tomen las medidas pertinentes. La presentación de la dinámica de la investigación fue realizada en la universidad de valencia España, donde el aporte a la implementación es conocer la estructura de un IDS basado en red, las ubicaciones antes y después del firewall, como analizan el tráfico, por qué se deben utilizar y sus desventajas.

Garzón Padilla, [19] en la implementación de un sistema de detección de intrusos (IDS) en la dirección general sede central del instituto nacional penitenciario y carcelario INPEC “pidsinpec, busca Reconocer las fallas de seguridad en la que actualmente la red de comunicación de la dirección General Sede Central del INPEC para determinar la ubicación de la instalación del IDS en la red. Es un antecedente de estudio porque se puede tomar como referencia desde lo conceptual y metodológico y me brinda un gran apoyo contemplado es su arquitectura y todo lo relacionado con el sistema.

González Gómez, [20] en su libro electrónico nos presenta un sistema de detección de intrusos en su versión 1.01 de la universidad de Deusto de España. La enorme

[18] MIRA ALFARO, Emilio José. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Proyecto Final de Carrera. Valencia – España. Universidad de Valencia. Facultad de Ingeniería. 2001. 42 p.

[19] GARZON PADILLA, Gilberzon. Propuesta para la Implementación de un Sistema de Detección de Intrusos en la Dirección General Sede Central del Instituto Nacional Penitenciario y Carcelario Inpec “pidsinpec”. Grado para Optar Título de Especialista en Seguridad Informática. Tunja. Universidad Nacional Abierta y A Distancia. ECBTI. 2015. 55 p.

[20] González Gómez, Diego. Libro Electrónico Sistemas de Detección de Intrusiones versión 1.01. Bilbao. Universidad de Deusto. 2003. 262 p.

variedad de grupos y propuestas de trabajo sobre las tecnologías de detección de intrusiones no hacen más que confirmar la importancia de la misma. Muchas empresas de seguridad han ratificado este hecho a través de la importancia de invertir para desarrollar sus propias soluciones basadas en los sistemas de detección de intrusiones

Britos, José Daniel, [21] El enfoque de este estudio se orienta al análisis y desarrollo de tecnologías basadas en la investigación estadística, las redes neuronales y los sistemas autónomos aplicados a los problemas de detección de intrusiones en redes de datos. La detección de intrusiones es una de las tareas más importantes y exigentes de la seguridad de las redes y el reconocimiento de patrones de ataques. Se ha abordado la detección de intrusiones con dos herramientas novedosas, las redes neuronales y las colonias de hormigas. En primer lugar, se comprueba que la red neuronal puede entrenarse fácilmente para distinguir entre condiciones normales y en condiciones de ataque de la red. Se obtuvo un error de aprendizaje de 0,56% y un error de generalización de 1,97%, utilizando una configuración sencilla de la red neuronal (configuración "back-propagation" con sólo dos neuronas en la capa oculta). Este resultado se ha logrado por el uso del módulo procesador estadístico que colabora en forma eficiente en la detección de intrusiones.

4.2 MARCO CONTEXTUAL

La ferretería Corintios es un establecimiento comercial dedicado a la venta de herramientas y objetos carpintería y herrería, como clavos, tornillos, alambres etc., La construcción y las necesidades del hogar, normalmente es para el público en general. Está ubicado en el barrio Líbano, de la comuna 9 de Santa Marta, estrato 2, sus habitantes en la mayoría son empleados que pertenecen a empresas privadas con un desempeño en el área operativo dentro de la ciudad.

Desde el año de 2006 Olga Tamara se dedicaba como empleada del gremio ferretero en la comercialización de sus artículos, tuvo la idea de crear su propia empresa con el objetivo de ejercer y fortalecer los conocimientos adquiridos durante el proceso de la empresa para la cual laboraba. La idea inicio surgiendo con la profundización del tiempo completo en el análisis del mercado donde se incluyeron las primeras líneas de los productos, proveedores para satisfacer las necesidades de sus clientes en la ciudad de santa marta. La primera ubicación de la empresa fue en un garaje alquilado para el almacenamiento de los artículos que en su momento

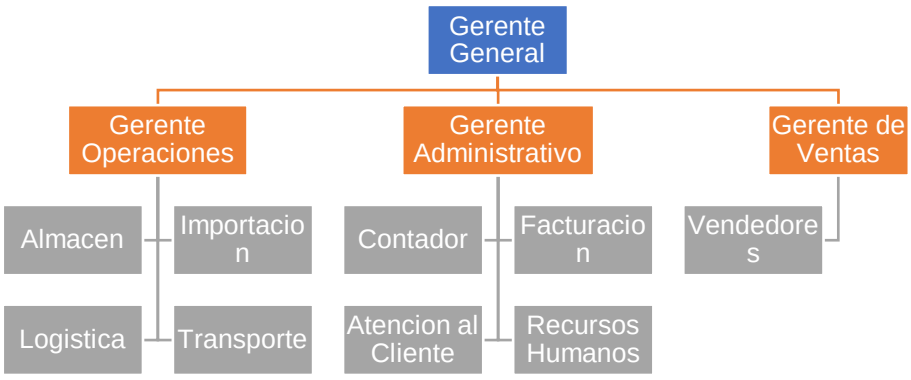
[21] BRITOS, José Daniel, Detección de Intrusiones en redes de datos con captura distribuida y procesamiento estadístico. Tesis de Maestría en Redes de Datos. Buenos Aires. Universidad Nacional de la Plata. 2010. 34 p.

eran los solicitados por sus primeros clientes. Durante la estadía en la capital magdalenense y el crecimiento en su base de clientes se inicia en las labores de logística que condujeran a encontrar el sitio adecuado para el montaje y definitivo sitio para seguir con el crecimiento. Al finalizar el año en curso (2006), se lleva a cabo la negociación que se concluye con la adquisición de una casa con su respectivo local ubicado en la urbanización Corintio Mz A Casa 29; a partir de ese momento se inicia la adecuación del local y el 2 de enero del 2007 comercializadora Corintio Abre sus puertas al público. Cabe resaltar que la determinación de escoger el nombre comercial de la ferretería y el lugar fue por la ubicación y que en su momento no se contaba con este servicio en el sector. En ese entonces se inicia labores con solo dos personas, un surtido modesto de productos el cual eran de los primeros clientes y después se fue adecuando acorde a la demanda de los clientes. Al pasar el tiempo la idea se fue formalizando como ferretería porque las demandas en la línea de los productos se fueron incrementando las ventas por mostrador sino la venta al por mayor por mostrador, ofreciendo un llamativo precio con respecto a las demás ferreterías de los sectores aledaños, el cual surge en el sector del barrio corintio y el vecino barrio Líbano 2000, se establece como Ferretería Corintios. Por esto se deja la comercialización de los productos a las ferreterías en santa marta y se atiende a los vecinos del sector y lugares aledaños; también incrementa el número de empleados y colaboradores.

La ferretería hoy en día cuenta con el fortalecimiento de sus líneas de productos de calidad, a precios bastantemente cómodos y competitivos, con la mejor atención prestada a sus clientes, haciendo que estos queden satisfechos con el buen servicio brindado. El crecimiento sigue hoy por hoy sigue creciendo dentro del mercado samario.

4.2.1 Organigrama

Figura 1Organigrama.



Fuente: Establecimiento Ferretería Corintio

4.2.2 Misión

Ser una empresa que trabaja para brindar a sus clientes la mayor diversidad en materiales de construcción y de ferretería en general, bajo premisas de precio, calidad y servicio acorde al crecimiento del mercado, con la intención de producir un incremento rentable, en comisión de todos que nos permita mantener y mejorar cada día la calidad y servicio prestado.

4.2.3 Visión

Mantener un sólido posicionamiento y liderazgo comercial en cuanto a la venta de materiales de construcción y ferretería en general, superando las perspectivas de calidad y servicio de nuestros clientes, gracias al apoyo absoluto de un gran equipo de trabajo, proporcionar el sostenimiento en un alto grado de responsabilidad social y comercial que nos garantice solidez financiera y crecimiento sostenible.

4.3 MARCO CONCEPTUAL

Para el desarrollo de este proyecto es necesario profundizar y estudiar todos los componentes que incluyan la conceptualización de la puesta en marcha e implementación y organización de un sistema de detección de intrusos.

4.3.1 Definición de intrusión

Una intrusión es un conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de algún recurso de nuestro equipo[22].

4.3.2 Historia de los IDS

Los primeros sistemas de detección de intrusiones fueron emergiendo a medida que el número de ordenadores crecía. Cuantos más ordenadores había más aumentaba

[22] VIÑES, Sanjuan Vanessa. Análisis de sistemas de detección de intrusiones. Proyecto Fin de carrera Ingeniería Técnica en Información de Sistemas. Cataluña, España. Universitat Rovira i Virgili. Facultad de Información de sistemas, 2005, 5 p

el número de eventos d sistema a analizar, era tal esta tarea que se volvió humanamente imposible de realizarla. Las autoridades militares de Norteamérica se dieron cuenta de que el uso cada vez más masivo de ordenadores en sus instalaciones requería algún mecanismo que facilitara la labor de sus auditores.

James P. Anderson fue la primera persona capaz de documentar la necesidad de un mecanismo que automatizara la revisión de los eventos de seguridad. Describió el concepto de "Monitor de referencias" en un estudio encargado por las Fuerzas Aéreas de EEUU, y redactó un informe en 1980 que sería el primero de los futuros trabajos sobre la detección de intrusiones. Uno de los objetivos de este informe era la eliminación de información redundante o irrelevante en los registros de sucesos. Anderson propuso un sistema de clasificación que diferenciaba entre ataques internos y ataques externos, basado en si los usuarios tenían permiso de acceso o no al ordenador.

Estos eran los principales objetivos de los mecanismos de auditoria de seguridad:

- Debían proporcionar suficiente información para que los encargados de seguridad localizaran el problema, pero no para efectuar un ataque.
- Debía ser capaz de obtener datos de distintos recursos del sistema.
- Para evitar ataques internos, debía detectar usos indebidos o fuera de lo normal por parte de los usuarios.
- El diseño del mecanismo de auditoria debía ser capaz de obtener la estrategia usada por el atacante para entrar en las cuentas.

Ideó un sistema para dar solución al problema de los intrusos que se habían apoderado de cuentas basándose en patrones de uso, creados a partir de análisis de estadísticas de comportamiento de usuario[23].

4.3.3 ¿Qué es un sistema de detección de intrusos?

Con el apoyo de la enciclopedia Wikipedia [24] se define como sistema de detección de intrusos "Es un Programa de detección de acceso no autorizado a un computador o a una red". En otras palabras, es una herramienta de seguridad que se encarga

[23] VIÑES, Sanjuan Vanessa. Análisis de sistemas de detección de intrusiones. Proyecto Fin de carrera Ingeniería Técnica en Información de Sistemas. Cataluña, España. Universitat Rovira i Virgili. Facultad de Información de sistemas, 2005, 6 p

[24] WIKIPEDIA. Sistema de detección de intrusos. [En Linea]. 06, Noviembre, 2017. 1 p. disponible en: https://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos

de verificar los eventos de los sistemas de información en busca de cualquier intento de intrusión.

4.3.4 IDS (Intrusion Detection Systems)

Anderson, James.[25] Es su reporte el día 26 de febrero de 1980, “Amenaza de Seguridad Informática Monitoreo y Vigilancia”, nos informa sobre la Penetración, como un ataque exitoso, la capacidad de obtener información no autorizada (no detectado) acceso a archivos y programas o al estado de control de un sistema de computadora. Donde el objeto a mejorar en su tiempo es la capacidad de auditoria y vigilancia de la seguridad informática de los sistemas del cliente. Con el apoyo del documento se puede deducir de la importancia para el desarrollo de los sistemas de detección de intrusos.

4.3.5 ¿Porque utilizar un IDS?

La protección a nuestros sistemas contra ataques, mal uso o adecuado compromete las organizaciones donde el principal patrimonio en la información. Con la utilización de un IDS se podrá proteger, implementar reglas y prevención en la conectividad en la red.

Los IDS con el transcurrir de los años se han ganado la aceptación de los ingenieros que se especializan contra la seguridad de la información y vulnerabilidades dentro y fuera de las compañías. Contemplando el respaldo para implementar políticas, cultura de seguridad para una mayor efectividad de los recursos tecnológicos implementados en los momentos especiales.

4.3.6 Características

Las principales acciones de los sistemas de detección de intrusos IDS, son aquellos sistemas encargados de localizar y responder de forma mecanizada ante los sucesos de seguridad que se presenten en la red y equipos informáticos.

Un origen de información que suministra sucesos del sistema o red informática.

[25] ANDERSON, James. Computer security threat monitoring and surveillance. [En Línea] Fort Washington, Pa. February 26, 1980. 6 p. Disponible en:https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf

Una base de datos de patrones de comportamientos considerados como normales, así como el perfil de distintos ataques.

Un propulsor de análisis apoderado de detectar evidencias de intentos de intrusos.

Repetición: son las encargadas para la detección de ataques específicos, donde permite a los administradores de diferencias de nuevos ataques cibernéticos.

4.3.7 Implementación de un sistema de detección de intrusos.

Es muy importante la implementación de la herramienta del sistema de detección de intruso porque permite a tiempo a las organizaciones de proteger todos sus sistemas de las amenazas que incrementan en la conectividad de la red y de los sistemas de información que en ella están. Con la interconexión con la red a nivel mundial o por medio de la www, hace que las empresas sean más vulnerables y están disponibles para cualquier ataque que se origine en su momento.

La respuesta a la implementación es la principal herramienta de minimizar en la infraestructura la seguridad que se necesita para cualquier organización. La herramienta no ayudara y tiene la capacidad de alerta de cualquier ataque que sea de origen interno o externo. Se previenen cualquier inconveniente para proteger o bloquear los ataques posibles, para poder determinar e identificar el ataque para que se pueda denunciar.

La mayoría de las organizaciones en sus sistemas operativos no tratan de actualizarse y por ende se genera en el área lo que se llama obsoleto donde no se pueden actualizar o renovados, generando una debilidad para los administradores y el poco apoyo económico de la alta gerencia porque se ve como algo de ultimo recursos y se sabe que día a día en lo que más se utiliza para los usuarios. En muy delicado cuando un ambiente que incluye un gran número de máquinas para sus posibles actualizaciones estos generan todo tipo de errores en sus configuraciones del sistema.

La herramienta en este capítulo del proyecto es de muy gran apoyo en la seguridad de la información de los sistemas computacionales.

4.3.8 Clasificación de los sistemas de detección de intrusos.

Mira Alfaro[26], nos presenta una clasificación de los sistemas de detección de intrusos que se presentan a continuación tabla 1:

Tabla 1 Clasificación de los Sistemas de Detección de intrusos

Clasificación	Tipos
Fuente de Información	IDS Basados en red (NIDS)
	IDS Basados en Host (HIDS)
Tipo de Análisis	Detección de abuso o firmas
	Detección de anomalías
Repuesta	Repuesta pasiva
	Repuesta Activa

Fuente: http://www.rediris.es/cert/doc/pdf/ids-uv.pdf

4.3.9 Tipos de Errores

Básicamente dos tipos de errores que puedan ocurrir en un sistema de detección de intrusos se pueden categorizar como:

- Falsos positivos: Es un término aplicado a un fallo de detección en un sistema de alertas. Sucede cuando se detecta la presencia de una intrusión en el sistema que realmente no existe.
- Falsos negativos: es un término que hace referencia a un fallo en el sistema de alertas. Sucede cuando un intruso intenta acceder a nuestro sistema y se le es permitida la entrada por el sistema de alertas[27].

La familia de los falsos positivos la podemos agrupar en cinco tipos, dependiendo de la naturaleza de su origen:

- Reactionary traffic alarms: Se detecta un comportamiento sospechoso como consecuencia de tráfico generado anteriormente. Por ejemplo, la detección

[26] MIRA ALFARO, Emilio José. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Proyecto Final de Carrera. Valencia – España. Universidad de Valencia. Facultad de Ingeniería. 2001. 18 p.

[27] VIÑES, Sanjuan Vanessa. Análisis de sistemas de detección de intrusiones. Proyecto Fin de carrera Ingeniería Técnica en Información de Sistemas. Cataluña, España. Universitat Rovira i Virgili. Facultad de Información de sistemas, 2005, 20 p

de muchas respuestas procedentes de un router porque el equipo destino no se encuentra operativo en esos momentos.

- Equipment-related alarms: Las alarmas del NIDS detectan paquetes dentro del tráfico de la red que identifica como “no usuales”.
- Protocol Violations: Estos avisos se producen por software mal programado o que implementan de forma incorrecta algunas partes de los protocolos de Internet.
- True False Positives: Todos aquellos falsos positivos que no se encuadren en ninguna de las categorías anteriores.
- Non Malicious Alarms: Alarmas producidas al detectar rastros de comportamientos maliciosos pero que en ese contexto determinado no lo son.

Los ejemplos de falsos negativos son más difíciles de detectar, generalmente suelen producirse por:

- Configuración deficiente de los recursos de la red: Por muchos elementos de seguridad que posea la red, esto no implica que sea segura. Si estos elementos están mal configurados, no podemos asegurar la red.
- Ataques desde dentro: Para intentar evitar eso se tendrían que tener controles internos para poder detectar a este tipo de atacantes.
- Equipos no parcheados y víctimas de los últimos “exploits”: Se tiene que intentar tener el equipo totalmente actualizado, de lo contrario el sistema será propenso a ser atacada.

4.3.10 Modelo IDS

El IDS puede utilizar dos modelos de detección:

- Detección de un mal uso: Tipo ilegales de tráfico, cadenas utilizadas para ejecutar ataques contra los exploits, escaneo de puertos.

- Detección de uso anómalo: Estudio estadístico del tráfico de la red, monitoreo de procedimientos y del comportamiento de los usuarios, con el fin de poder detectar aquellas prácticas que se pueden considerar anómalos según la guía de usos registrados hasta el momento.

Con la efectividad de los módulos de los IDS con la rapidez de respuesta, son capaces de actuar de forma automática a los incidentes detectados.

Los sistemas de detección de intrusos presentan una limitaciones y problemas, como podrían ser la generación de falsas alarmas, ya sean falsos negativos, que se produce con IDS no es capaz de detectar alguna actividad relacionada con incidentes de seguridad que presenta la red o en los equipos informáticos, o bien los falsos positivos, que se producen cuando el IDS registra y genera alertas sobre determinadas actividades que no resultan tan problemáticas, ya que forman parte de las actividades o funcionamiento normal del sistemas o red informático.

4.3.11 Métodos de detección

Los sistemas de detección de intrusos utilizan cuatro métodos de detección:

- Basados en firmas, anomalías estadísticas basadas en el protocolo y el análisis de estado.

- Detección justificada en firmas: Este procedimiento de detección emplea firmas, que son las guías de ofensiva que están preconfigurados y predeterminada. Estas reglas se relacionan con el paquete capturado y si no satisface con los lineamientos de inmediato se impide el acceso.

- Anomalía basada en registros de detección: Negociar este método los IPS crean una fila base que representa la labor común de los usuarios, normalmente cuando existe un ataque el sistema detecta una derivación de la práctica normal de la red y originar la acción.

- De estado de detección de estudio de protocolo: Este método establece las derivaciones del protocolo cotejando los encabezados de los paquetes y apropiarse la acción si no satisface con los parámetros que lo identifican

4.3.12 Herramientas y complementos

4.3.12.1 Sistemas de valoración y análisis de vulnerabilidades

Las herramientas de análisis de vulnerabilidades determinan si una red o host es vulnerable a ataques conocidos. La valoración de vulnerabilidades representa un caso especial del proceso de la detección de intrusiones. Los sistemas que realizan

valoración de vulnerabilidades funcionan en modo ’batch’ y buscan servicios y configuraciones con vulnerabilidades conocidas en nuestra red.

4.3.12.2 File Integrity Checkers (Controladores de la integridad de los ficheros)

Los ’File Integrity Checkers’ son otra clase de herramientas de seguridad que complementan a los IDS. Utilizan resúmenes de mensajes (message digest) u otras técnicas criptográficas para hacer un compendio del contenido de ficheros y objetos críticos en el sistema y detectar cambios, de tal forma que para cualquier cambio del contenido del fichero el compendio sea totalmente distinto y que sea casi imposible modificar el fichero de forma que el compendio sea igual al del fichero original[28].

El uso de estos controladores es importante, puesto que los atacantes a menudo alteran los sistemas de ficheros una vez que tienen acceso completo a la máquina, dejando puertas traseras que más tarde facilitan su entrada al sistema, esta vez "sin hacer tanto ruido".

El producto Freeware Tripwire (www.tripwiresecurity.com) es quizá el ejemplo más conocido de este tipo de herramientas.

4.3.13 Honeypots

Son sistemas que están diseñados para ser atacados y que capturan de forma silenciosa todos los movimientos del atacante. Se usan principalmente para lo siguiente:

- Evitan que el atacante pase su tiempo intentado acceder a sistemas críticos.
- Recogen información sobre la actividad del atacante.
- Permiten al administrador recabar pruebas de quién es el atacante y responda ante su CERT o el administrador del sistema origen de la agresión.

Los Honeypots se usan ampliamente para investigar sobre nuevos ataques, y facilitan la incorporación de nuevas firmas en los IDS.

[28] VIÑES, Sanjuan Vanessa. Análisis de sistemas de detección de intrusiones. Proyecto Fin de carrera Ingeniería Técnica en Información de Sistemas. Cataluña, España. Universitat Rovira i Virgili. Facultad de Información de sistemas, 2005, 22 p

4.3.14 Limitaciones IDS

Las limitaciones de los IDS en una actitud paranoica y de muy gran importancia para generar un problema es cuando queremos implementarlo en redes conmutadas ya que no hay segmentación de red por donde se pueda filtrar todo el tráfico que pase.

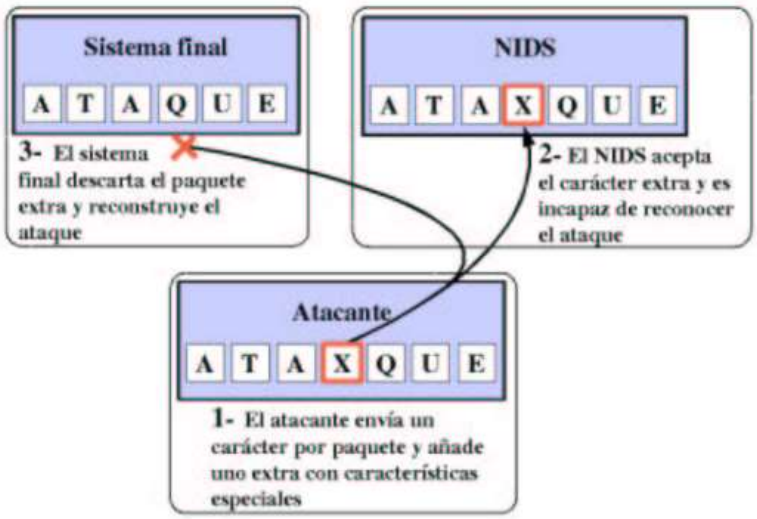
Otra de las limitaciones para los IDS son las redes con velocidades de tráfico muy altas en las cuales es difícil procesar todos los paquetes que se generan en el tráfico de las redes. Este conlleva que los IDS son incapaces de detener los ataques por sí solo sino hay reglas contempladas para la administración del filtro de captura para efectuar la mejor detección posible.

Sin embargo, los ataques anti-IDS que más estragos causan son los de ’inserción’ y ’evasión’, que veremos a continuación.

4.3.14.1 Inserción

El ataque de inserción se basa en que un IDS puede aceptar paquetes que luego un sistema final va a rechazar. La figura 2 da un ejemplo del ataque.

Figura 2 Ataque de Inserción



Fuente: https://www.rediris.es/cert/doc/pdf/ids-uv.pdf

Un atacante envía un flujo de un carácter por paquete, en el cual uno de los caracteres aparecerá solo en el IDS. Como resultado, el IDS y el sistema final reconstruirán dos cadenas distintas. En general, un ataque de inserción ocurre cuando el IDS es menos estricto en procesar un paquete que el sistema final. Una

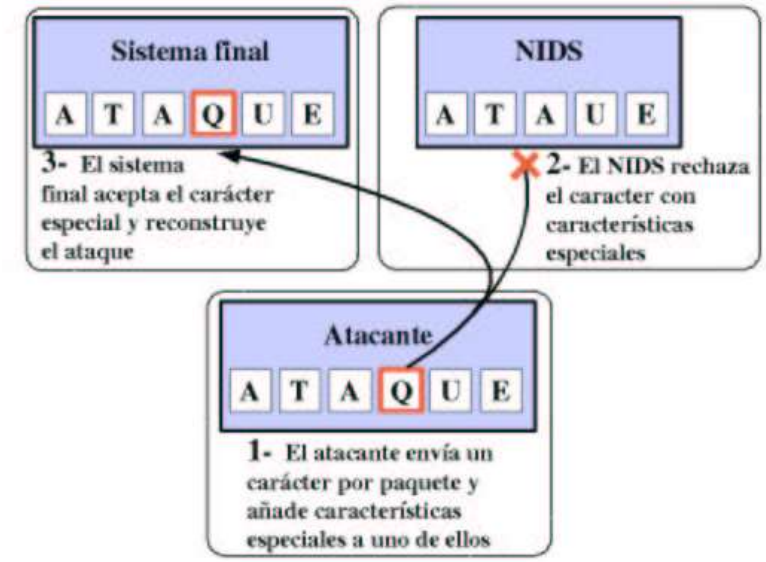
reacción obvia a este problema puede ser la de hacer al IDS tan estricto como sea posible en procesar paquetes leídos de la red; esto podría minimizar los ataques de inserción, Sin embargo, al hacer esto podemos estar dando facilidad a otro ataque, el de evasión, que veremos a continuación[29].

4.3.14.2 Evasión

Un sistema final puede aceptar un paquete que un IDS rechace. En la figura 1.6 podemos ver un ejemplo de este ataque:

El ataque de evasión provoca que el IDS vea un flujo diferente que el sistema final. Esta vez, sin embargo, el sistema final toma más paquetes que el IDS, y la información que el IDS pierde es crítica para la detección del ataque.

Figura 3 Ataque Evasión



Fuente: https://www.rediris.es/cert/doc/pdf/ids-uv.pdf

4.3.14.3 Solución definitiva

Los problemas de seguridad pueden originarse por múltiples motivos. No existe ninguna solución única que resuelva todos. Los sistemas de detección de

[29] MIRA ALFARO, Emilio José. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Proyecto Final de Carrera. Valencia – España. Universidad de Valencia. Facultad de Ingeniería. 2001. 42 p.

intrusiones no son una excepción. No obstante, aportan una serie de características únicas que los conviertan en herramientas de gran ayuda en muchos entornos[30].

4.3.14.4 Falsos positivos

Uno de los inconvenientes más populares entre la detección de intrusiones es el de falsas alarmas; falso positivos y falsos negativos. Los falsos positivos consisten en aquellas alarmas que tienen lugar cuando en realidad no se está produciendo ninguna intrusión[31].

4.3.14.5 Falsos negativos

Son uno de los tipos de falsas alarmas, y se producen cuando no se emite el correspondiente aviso cuando sucede realmente un ataque o intrusión. Este tipo de situaciones, por razones obvias, también representan un problema. Cuando un atacante utiliza una técnica nueva, un ataque modificado basado en alguno ya existente, un ataque especializado contra este tipo de sistemas, o cuando un detector de anomalías es entrenado de forma progresiva por un intruso, para que interprete una acción hostil como normal, son solo algunos ejemplos en los que pueden ocurrir falsos negativos[32].

4.3.14.6 Autosuficiencia

No pueden compensar las debilidades o ausencias de otros sistemas de seguridad de la infraestructura, como contraseña de baja calidad, cortafuegos, antivirus, etc.

---

[30] GONZALEZ, Gómez Diego. Sistemas de detección de intrusiones. Versión 1.01, España, Julio 2003 127 p.

[31] GONZALEZ, Gómez Diego. Sistemas de detección de intrusiones. Versión 1.01, España, Julio 2003 128 p.

[32] GONZALEZ, Gómez Diego. Sistemas de detección de intrusiones. Versión 1.01, España, Julio 2003 129 p.

4.3.14.7 Investigación automática

Realizan tareas de análisis y envían alarmas en caso de reconocer intrusiones o acciones hostiles. No obstante, es labor de investigación de cada ataque realizado la debe realizar un humano. Este tipo de acciones conlleva ciertas responsabilidades y habilidades de las que carecen estos sistemas[33].

4.3.14.8 IPv6

Muchos detectores de intrusiones comerciales son incapaces de interpretar el protocolo IPv6, sucesor del ampliamente utilizado en internet IPv4. El protocolo IPv6 no está siendo adoptado por el igual en todo el mundo, teniendo mayor acogida en los países asiáticos. Sin embargo, incluso en entorno en los que se trabaja únicamente con Pv4, el protocolo IPv6 permite crear túneles sobre la IPv4. Esto impide a los detectores de intrusiones reconocer aquellos ataques que lo utilizan. Esta situación se puede corregir añadiendo capacidades de análisis de este protocolo a los motores de detección.

4.4 PRODUCTO COMERCIALES IDS

4.4.1 Dragon - Enterasys Networks

El IDS de Enterasys Networks, Dragon [34], toma información sobre actividades sospechosas de un sensor denominado Dragon Sensor y de un módulo llamado Dragon Squire que se encarga de monitorizar los logs de los Firewalls y otros sistemas. Esta información es enviada a un producto denominado Dragon Server para posteriores análisis y correlaciones. Cada componente tiene ventajas que compensan con debilidades de otro, por ejemplo, el sensor Dragon Sensor es incapaz de interpretar tráfico codificado de una sesión web SSL, pero el producto Dragon Squire es capaz de recocer los logs del servidor web y pasárselos a la máquina de análisis. Veamos un poco más en detalle cada uno de estos componentes.

---

[33] GONZALEZ, Gómez Diego. Sistemas de detección de intrusiones. Versión 1.01, España, Julio 2003 130 p.

[34] MIRA ALFARO, Emilio José. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Proyecto Final de Carrera. Valencia – España. Universidad de Valencia. Facultad de Ingeniería. 2001. 34 p.

4.4.2 NetRanger - Cisco Systems

El sistema de detección de intrusos de Cisco, conocido formalmente por Cisco NetRanger[35] , es una solución para detectar, prevenir y reaccionar contra actividades no autorizadas a través de la red.

Cisco IDS Host Sensor v2.0 es capaz de identificar ataques y prevenir accesos a recursos críticos del servidor antes de que ocurra cualquier transacción no autorizada. Esto lo hace integrando sus capacidades de respuesta con el resto de sus equipos, como veremos más adelante.

La versión más reciente actualmente del sensor de cisco es la v3.0, que incluye un mecanismo de actualización automática de firmas, un lenguaje robusto que permite a los clientes escribir sus propias firmas y extensiones al módulo de respuestas que añaden soporte para la familia de firewalls Cisco PIX y para los conmutadores Cisco Catalyst.

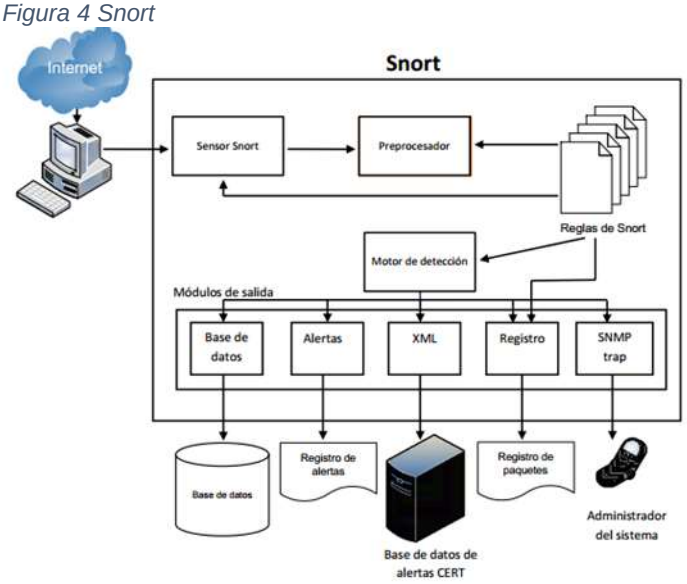
4.4.3 Snort

Sistema detector de intrusos, basado en red; una de la ventaja de este sistema también es que puede funcionar como un sniffer de verificación de paquetes; con esta función se puede ver desde consola en tiempo real lo que ocurre en una red todo el tráfico generado. Es una aplicación bajo licencia software GPL. Dispone de un lenguaje de creación de reglas en el que se definen los patrones que se deben utilizar a la hora de administrar el monitoreo de un sistema.

Las funciones más básicas del Snort es monitorear, detectar y responder ante los eventos sospechosos que puedan entrar y salir de cualquier compañía en todo el mundo. También está basado en las firmas que sean registradas en sus reglas de filtro.

[35] MIRA ALFARO, Emilio José. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Proyecto Final de Carrera. Valencia – España. Universidad de Valencia. Facultad de Ingeniería. 2001. 38 p

Figura 4 Snort



Fuente: http://catarina.udlap.mx/u_dl_a/tales/documentos/mcc/muniz_b_p/capitulo2.pdf, pagina23.

4.4.4 Shadow

Fue desarrollado como respuesta a los falsos positivos de un IDS anterior, NID. La idea era construir una interfaz rápida que funcionara bien en una DMZ caliente (una DMZ que sufre muchos ataques). La interfaz permitiría al analista evaluar gran cantidad de información de red y decidir de qué eventos informar.

No es en tiempo real. Los diseñadores de Shadow[36] sabían que no iban a estar disponibles para vigilar el sistema de detección de intrusos 7 días a las semanas, 24 horas al día. Shadow almacena el tráfico de red en una base de datos y se ejecuta por la noche. Los resultados esperan a que el analista llegue a la mañana siguiente.

Al no ser en tiempo real, es inviable que Shadow analice el contenido de los paquetes, por lo que tan solo se centra en las cabeceras. Esto le hace inútil para análisis forense.

[36] MIRA ALFARO, Emilio José. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Proyecto Final de Carrera. Valencia – España. Universidad de Valencia. Facultad de Ingeniería. 2001. 44 p.

4.5 MARCO LEGAL

Para nuestro país existe un procedimiento legal, donde el ministerio de tecnologías y las comunicaciones de Colombia. (MINTIC), por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos", cuya función es preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones entre otras disposiciones. El proyecto se fundamenta en la ley 1273 de 2009 [37] , donde se ejecutará acorde con las normas y requisitos legales de la actualidad.

Se clasifican los delitos informáticos en Colombia a continuación que afectan la seguridad de la información.

- Art. 269 C.

Interceptación de datos informáticos. Se cometen cuando se obstruyen datos sin autorización legal, durante la trasmisión de datos ente un remitente y receptor. Tiene una pena de 36 a 72 meses de prisión.

- Art. 269 D.

Daño informático. El individuo que interfiere en el cambio de estado de un elemento que contiene información, el cual cambie o incluso elimine, esto constituye una conducta delictiva.

- Art. 269 E.

Uso de Software Malicioso. El software malicioso empleados para la obtención de los sistemas de información donde se pueda copiar o de igual manera extraer; este procedimiento genera una serie de daños en los medios tecnológicos e informáticos por la pérdida de información muy importante o delicada.

[37] COLOMBIA. MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Ley 1273 (5, Enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Bogotá: El Ministerio, 2009. 2 p

- Art. 269 F.

Violación de datos personales. El enviar, tomar y sustraer información privada de un sistema de información, con fines personales o para beneficiar otras personas a cambio de un beneficio económico u otra razón comete un delito.

- Art. 269 G.

Suplantación de sitios web para capturar datos personales. Crear una página o sitio en la web side 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.

5 METODOLOGIA DE DESARROLLO

5.1 FASE I ESTADO DE LA INFRAESTRUCTURA

Uno de los ítem y recursos del proyecto fue la información poca que se dispone actualmente la ferretería corintio con respecto a la administración de la misma como área de sistema y de la poca inversión sobre esta.

El procedimiento que se utilizó para la realización del proyecto y sus prácticas en sitio donde se realizó como diario el registro en el proyecto donde se realiza la captura de la pantalla de los procedimientos realizados y el detalle de la observación directa para verificar las condiciones con las que se encuentran los sistemas de la ferretería corintio que es la empresa donde se realiza el proyecto y entregar a satisfacción con el cliente.

Para el planteamiento y estructura del proyecto se da como inicio como base los objetivos que se plantean en el proyecto y a la vez de ir plasmando la información de los procedimientos generados para contribuir de la solución de cada objetivo plateado en el proyecto. El cumplir a cabalidad con cada uno de los cuatro objetivos arrojo los resultados finales que ayudan a enriquecer los conocimientos aprendidos en el transcurso de la misma. A continuación, se detalla por fases todo el desarrollo y resultados de los objetivos específicos.

5.1.1 ESTADO DE INFRAESTRUCTURA Y CONFIGURACIÓN DE RED

La Ferretería Corintio actualmente está conformada con una sola sede principal en la ciudad de Santa Marta (Magdalena), donde se encuentra toda su operación comercial.

La infraestructura de equipos encontrados en sitio.

Tabla 2 Infraestructura de Equipos

HARDWARE	CANT	DESCRIPCION
PC Servidor_Archivo	1	Pc se utiliza para el almacenamiento de la información de la ferretería.
Pc	6	Equipos de Trabajo de la ferretería.
Switch D-Link	1	Equipo de Comunicación entre su Red LAN.
Modem ADSL	1	Servicio ISP - Movistar

Fuente: Autor

5.1.2 Esquema del Hardware y software

El esquema de su infraestructura en hardware y software con el que cuenta la ferretería corintio en este momento es de siete (7) pc de fabricación Clon, basados en el diseño y desarrollo de otras compañía en el interior de la máquina; el software se divide en tres (3) con sistema operativo home Basic de cada pc está basado en un sistema operativo Windows 7 home Basic de arquitectura versión a 32 bit; uno (1) con sistemas operativo Home Basic basado en un sistema operativo 7 Home Basic de arquitectura a 32 bit, tres (3) con sistema operativo Windows XP profesional service pack 2 sobre la versión a 32 bit.

A continuación, se detalla el esquema del hardware que se encuentra en sitio de la ferretería corintios en la actualidad.

Se encuentra tres (3) pc que presentan el sistema operativo Home Basic con arquitectura versión a 32 bit tienen las siguientes características del hardware.

Tabla 3 Descripción hardware windows basic home

SOFTWARE	DESCRIPCION	HARDWARE	DESCRIPCION
OS	Windows Basic Home a 32Bit	Procesador	Intel Celeron dual Core 2,41 Ghz
		Board	integrada Biostar (a,v,r, hdmi)
		Memoria	2gb
		Disco Duro	500gb sata
		Keyboard	Genius
		Unidad Lectora	Rw-Dvd
		Fuente	Atx Fuente 300w
		Pantalla	Lcd 17“ 1280*800

Fuente: Autor

A continuación, se describe el hardware de tres (3) pc que cuentan con un sistema operativo Windows XP, una revisión visual, su estado actual y las condiciones en la que se encuentran.

Tabla 4 Descripción Hardware Windows XP Profesional

SOFTWARE	DESCRIPCION	HARDWARE	DESCRIPCION
OS	Windows XP Professional service pack 2 a 32 Bit.	Procesador	Intel Celeron dual Core 1,8 Ghz
		Board	integrada Biostar (a,v,r, hdmi)
		Memoria	1,5gb
		Disco Duro	320 Gb sata
		Keyboard	Genius
		Unidad Lectora	Rw-CD
		Fuente	Atx Fuente 300w
		Pantalla	Lcd 17 " 1280*800

Fuente: Autor

Se describe el hardware de un (1) pc que se encuentran trabajando como servidor de archivos con un sistema operativo Home Basic arquitectura a 32 Bit.

Tabla 5 Descripción Hardware Servidor Archivo

SOFTWARE	DESCRIPCION	HARDWARE	DESCRIPCION
OS	Windows Basic Home a 32Bit	Procesador	Intel Celeron dual Core 2,41 Ghz
		Board	integrada Biostar (a,v,r, hdmi)
		Memoria	4gb
		Disco Duro	500gb sata
		Keyboard	Genius
		Fuente	Atx Fuente 300w

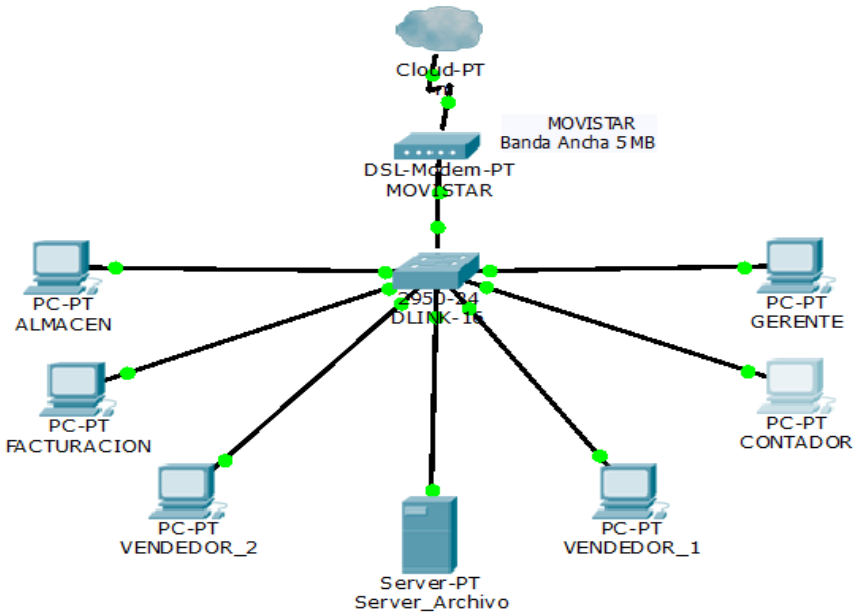
Fuente: Autor

5.1.3 Esquema de seguridad de la red

En este momento no cuenta con ningún sistema de seguridad de red. Lo único que se tiene es el modem ADSL que es suministrado por un proveedor de servicios de internet (ISP), que es la que brinda a la empresa la conexión a internet que se llama

Movistar. La Ferretería Corintio no dispone de un diagrama de red. Al no encontrar información con respecto a la estructura de la red, se procedió a realizar un levantamiento físico en las instalaciones para determinar cuál es la topología a su vez se entenderá de la mejor forma en que los equipos terminales se conectan entre sí. A continuación, se presenta por medio de la herramienta de packet tracer el diagrama.

Figura 5 Diagrama de Red Actual



Fuente: Autor

Se puede determinar que se cuenta con una estructura de red estrella. Porque se encuentra como nodo central un switch de 16 puertos marca D-Link; y conectados todas las terminales y que actúa como el distribuidor del tráfico que generado de las comunicaciones.

5.1.4 Levantamiento de tipo de información a proteger.

Luego de revisar la cantidad y tipo de información que se maneja en la red de la ferretería corintios, se puede evidenciar que la principal información de carácter urgente es la información que se guarda en el servidor de archivos, donde están alojados los tipos de documentos como facturas por cancelar, facturas por entregar, inventario de los materiales y artículos, la base de datos que se maneja en Excel de los clientes y proveedores, listado de precios, la contabilidad desde que la ferretería inicio hasta la fecha, las cuentas por cobrar, los créditos que se suministran a los clientes ya sea por mostrador, ferreterías. Cabe recalcar la importancia de la

información que se almacena y procesa a diario. Donde no se lleva un control y verificación a continua.

Tabla 6 Clasificación de Información por área

AREAS	DESCRIPCION
CONTABILIDAD	• Información Financiera. • Pagos de Impuestos. • Balance financiero • Cuentas Por Pagar • Cuentas por Cobrar
ALMACEN	• Inventarios. • Activos. • Documentación de Vehículos.
GERENCIA	• Estado de Perdida y ganancia. • Indicadores de Venta • Informe Contable. • Auditorias. • Contratos. • Contratación de Personal.
VENTAS	• Indicadores de Venta. • Estado de cuentas de Vendedores
FACTURACION	• Listado de Precios. • Listados de Clientes • Listado de Stock. • Estado de Cuenta. • Cuentas por Cobrar. • Cuentas por Pagar.

Fuente: Autor

5.2 FASE II PROVISIONAR DE HERRAMIENTAS TECNOLOGICAS.

Después de la verificación visual se determina que la ferretería corintio se necesita con urgencia, en ejerció del procedimiento que nos otorga los software de licencia gratuita y sin la inversión económica de la misma para dar soluciones que conlleven a la buenas prácticas que como principios se deben cumplir y demostrando con la

generación de un informe general de la herramienta como apoyo a la verificación de la información que se transporta por medio de la red.

Para el desarrollo de este objetivo y por falta de presupuesto se escoge entre los más populares como herramienta y a su vez como gratuito o de software libre se menciona a lo largo del proyecto el Snort como sistema para detección de intrusos y la confidencialidad de la información que se suministra y se transporta por la red local.

La herramienta tecnológica para el desarrollo del proyecto en la implementación en el sistema de detección de intrusos con el que se establece es Snort. La herramienta es muy importante para la seguridad perimetral en cualquier ambiente. Con el Snort me permite controlar todo el tráfico en tiempo real de la red en la cual se realizará la instalación. Estos paquetes serán análisis por medio de su consola y en tiempo real donde se implementa un motor de detección de ataques y escaneo de puertos que permite registrar todas las alertas y responder ante cualquier anomalía previamente definida.

5.2.1 Inventario de Herramientas Tecnológicas Encontradas

Las herramientas tecnológicas con las que cuenta la ferretería corintios, para determinar el inicio del proyecto para el analice de la propuesta de implementación de un sistema de intrusos en le red, es un pc que se llama servidor de archivo donde se puede trabajar y realizar las pruebas de la implementación de un sistema de detección de intrusos

5.2.2 Elementos Tecnológicos para la Implementación de IDS

Se realiza las recomendaciones a la gerencia que las pruebas a realizar de la implementación de un sistema de detección de intrusos con el software Snort basado licencia GPL (Licencia Gratuita), debe ser en un equipo solo disponible para el ejercicio. Por la implementación se realizará el montaje en un entorno virtual y posteriormente se estaría migrando la maquina a un entorno físico después de realizar las pruebas y resultados obtenidos durante la ejecución del proyecto; para después ser incluido dentro del nuevo presupuesto para el área de tecnología. Teniendo en cuenta que en el ambiente virtual la empresa tiene sus aplicaciones en producción por temas de espacio y costos.

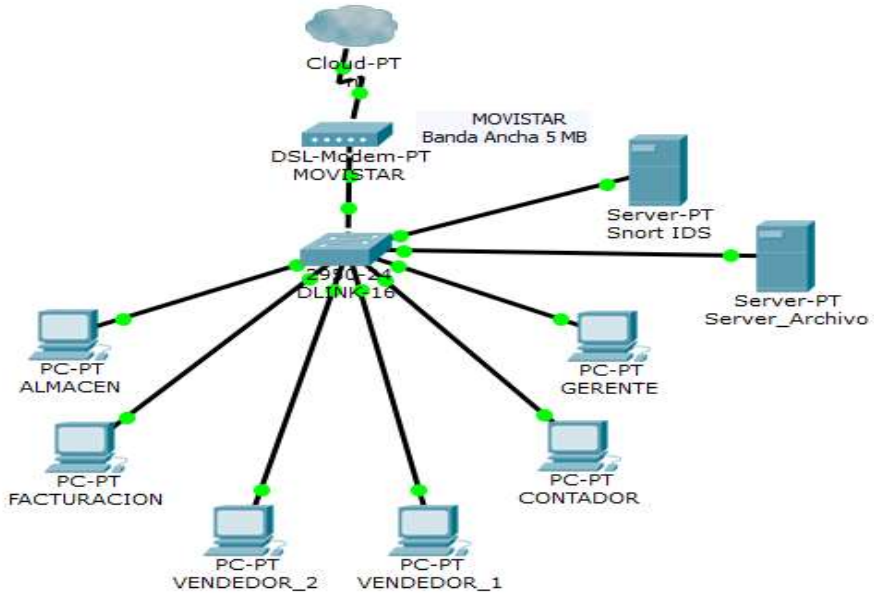
Para darle una mayor protección del equipo donde se instalará la máquina virtual, se van a mencionar algunas recomendaciones antes de la instalación del sistema de detección de intrusos como son las siguientes:

- Limitar acceso físico. Es colocar el Snort en un área segura, accesible solo al personal autorizado en este caso al especialista en seguridad informática que está desarrollando el proyecto a su implementación.
- Instalar los componentes necesarios para el funcionamiento del sistema operativo.
- Deshabilitar protocolos de red no necesarios.
- Habilitar solo lo servicios que se van a utilizar en la máquina.
- Realizar actualizaciones de seguridad, parches y aplicarlos para que el sistema este actualizado.

5.2.3 Diseño e Instalación y Configuración

El IDS se coloca tras un switch donde se unen las conexiones y no altera las tramas que llegan.

Figura 6 Topología de red Diseño IDS



Fuente: Autor

5.2.4 Componentes de la instalación.

A continuación, se relaciona los componentes para el inicio e implementación del sistema de detección de intrusos en la ferretería corintios, son los siguientes:

- VirtualBox 5.1.18
- Máquina virtual con Sistema Operativo Windows 7 Professional 32 bits
- WinPCap 4.1.3
- Snort 2.9.9.0
- Snortrules-snapshot-2990
- Rule Documentation (opensource.tar.gz)
- Strawberry Perl 5.24.1.1
- MySQL Database 5.7.18.0
- PHP 5.6.29 NTS (VC11)
- IS 7.5 - included with Windows 7
- Create-sidmap
- Barnyard2-2.1.14
- ADODB-5.20.9
- dotNetFx40_Full_x86
- dotnetfx35setup
- Unzip
- test.php
- winids-cssp-x86

5.2.5 Requerimiento y aplicaciones.

Sistema operativo Windows 7 profesional, aunque la configuración de Snort corre en prácticamente en cualquier versión de 32 bits de Windows, pero para el ejerció del proyecto se trabajara con la versión inicialmente mencionada. Por ser muy estable y soporta más de un procesador.

Instalación de Máquina Virtual y VirtualBox.

Para la instalación del Snort, se necesitará instalar una máquina virtual en el pc que se utiliza como server_archivo, el software para realizar la virtualización para desarrollar el proceso de la implementación de un sistema de intrusos se llama virtualbox versión 5.1.18 descargable de la página: https://www.virtualbox.org/. Como se muestra en la figura 7.

Figura 7 Máquina Virtual Snort

Fuente: Autor

5.2.6 Instalación de Windows 7 Profesional.

Para la realización de las pruebas e instalación de la maquina donde se instalará el sistema de detección de intrusos que para este caso será Snort, bajo licencia GLP (Licencia Gratuita). Se instaló un sistema operativo Windows 7 profesional de arquitectura a 32 Bit. Como se muestra en la figura 8.

Figura 8 Windows 7 Profesional

Fuente: Autor

Las especificaciones de la máquina para poder soportar la instalación del sistema de detección de intrusos (Snort) y sus pruebas son las siguientes:

Tabla 7 Especificaciones Máquina Virtual Snort

SOFTWARE	DESCRIPCION	HARDWARE	DESCRIPCION
OS	Windows Profesional a 32Bit	Procesador	Intel Celeron dual Core 2,41 Ghz
		Board	integrada Biostar (a,v,r, hdmi)
		Memoria	2gb
		Disco Duro	120gb sata

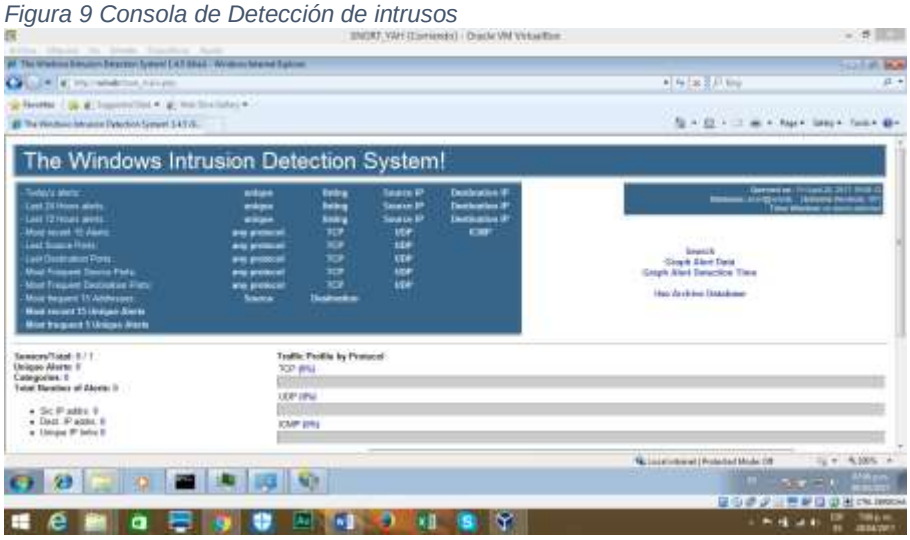
Fuente: Autor

5.2.7 Consola de IDS

Para realizar la prueba de inicio de consola del sistema de detección de intrusos se abra un navegador web y escriba http: // winids en el cuadro Dirección URL y pulse la tecla Enter.

Después del reinicio, los eventos pueden tardar varios minutos en comenzar a instalarse en la consola de seguridad del sistema de detección de intrusos. Actualizar el navegador mostrará nuevos eventos cuando se agrega.

Figura 9 Consola de Detección de intrusos



Fuente: Autor

5.2.8 Mantenimiento y Actualización

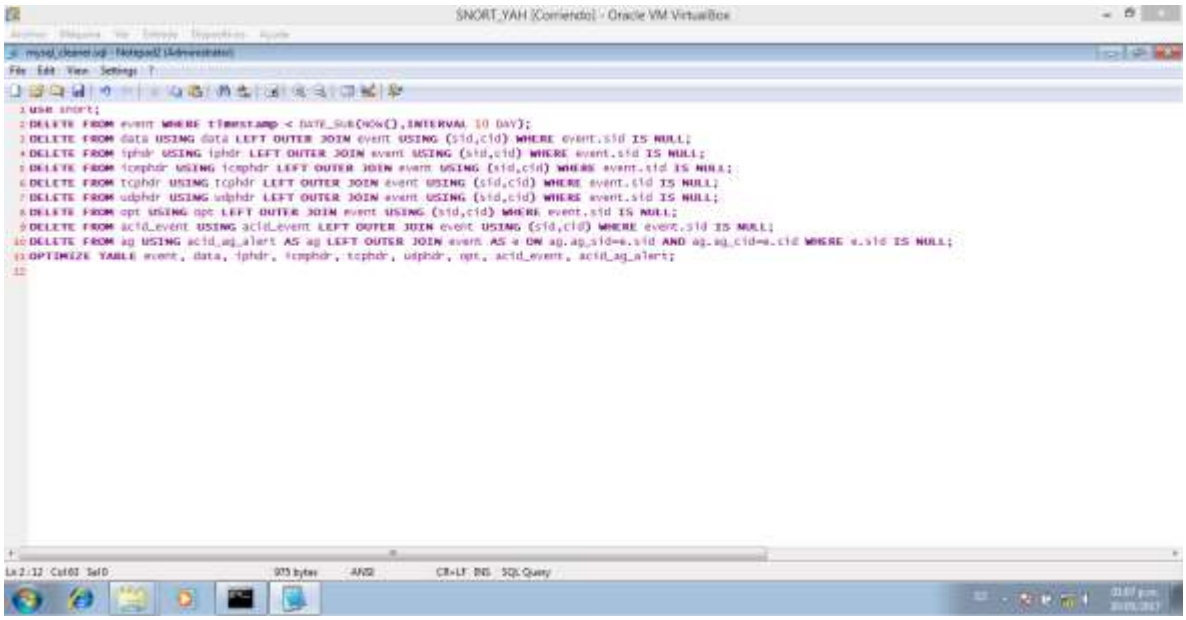
5.2.8.1 Limpieza de la Base de Datos MySQL del Sistema de Detección de Intrusos.

Para el procedimiento de limpieza en la administración de la base de datos MySQL de todos los registros generados por los sensores del sistema de detección de intrusos configurado por las reglas del Snort, se realizará una breve explicación de su limpieza.

Para ejecutar el procedimiento se debe ejecutar el script SQL denominado mysql_cleaner.sql, que se encuentra en la carpeta D:\temp. Con la ubicación del script SQL, se procede a ejecutar una ventana de CMD y se escribe notepad2 d: \ mysql_cleaner.sql, y se pulsa la tecla de enter.

La función para realizar del script SQl, es limpiar toda la información de los eventos almacenados en la base de datos, pero con una excepción que me permite solo salvaguardar los último días de los datos encontrados, para realizar el ejemplo se tomara como información de 20 días de datos del Snort. Al proceder con el script SQL por medio del programa Notepad2, me dirijo a la línea 2 donde se encuentra el siguiente código DELETE FROM event WHERE timestamp < DATE_SUB(NOW(),INTERVAL 28 DAY); y se cambia el 28, por 10 que son los días que se reflejan en el número de días de datos que se mantendrán en la base de datos. Como se muestra en la figura 10.

Figura 10 Línea de Comando



Fuente: Autor

Cuando ya ajusto los días de limpieza que se podrán guardar y mantener en la base de datos se procede a cerrar el programa de Notepad2.

5.3 FASE III DETERMINAR LOS CONTROLES QUE SE DEBEN ADOPTARSE EN CUENTO A LA CONFIGURACION Y ADMINISRACION DE LA RED.

Partiendo de la necesita que surge y los procedimientos para adoptarse en el rendimiento y seguimiento de toda la administración que se realice para el beneficio del proyecto y también para implementar las pautas necesarias y básicas para la propuesta a la implementación de un IDS.

Como medida de carácter muy importante se procederá a implementar políticas de seguridad con el fin de concientizar a los empleados que hacen parte de la Ferretería Corintio, al uso y apropiación de estas políticas generando un gran compromiso hacia la compañía.

5.3.1 POLITICAS DE SEGURIDAD

Con la definición de las políticas de seguridad de la información, establecidas por la ferretería Corintios se busca establecer en todos los pc y lo que se encuentre en la red, para promover una cultura de importancia realizándose de una forma confiable y eficaz.

La seguridad de la información es un procedimiento donde se deben determinar y administrar los riesgos, respaldarse en políticas que cubran las necesidades de la empresa en componente de seguridad.

Las políticas de seguridad de la información tienen por propósito establecer reglas y patrones técnicos de dirección y organización de las Tecnologías de Información y Comunicaciones TIC´s de todo el personal comprometido en el uso de la prestación informática conforme por el área de seguridad informática de la Ferretería Corintios.

5.3.2 Seguridad Corporativa.

Toda persona que ingresa como usuario nuevo a la ferretería Corintios, para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas por la gerencia.

5.3.3 Nuevos Usuarios.

Es responsabilidad de la gerencia cumplir las Políticas y Estándares de Seguridad Informática y manifestar la obligatoriedad de la misma.

Los nuevos usuarios serán creados únicamente por la alta gerencia, según el perfil y el nivel de acceso requerido para cada cargo, estos serán creados en el directorio activo, donde se aplicarán las políticas de seguridad.

Para gestionar correctamente la seguridad de las contraseñas se deben cumplir las siguientes políticas y acciones:

- Se deben utilizar al menos 8 caracteres para crear la clave.
- Se debe utilizar en una misma contraseña con dígitos, letras y caracteres especiales.
- No debe contener una palabra completa.
- Debe ser elocuentes y diferente de otras contraseñas anteriores.
- No deben llevar el nombre de usuario, el nombre real o el nombre de la empresa.

5.3.4 Capacitación en Seguridad informática y seguridad de la información.

Todo funcionario nuevo en la ferretería Corintios deberá contar con la inducción sobre las Políticas y Estándares de Seguridad de la información, donde se den a conocer las responsabilidades para los usuarios y castigar en que pueden incurrir en caso de incumplimiento.

5.3.5 Sanciones.

Se considera violación grave la divulgación de información reservada o confidencial de la ferretería corintios.

5.3.6 Protección de la Información y de los bienes Informáticos.

El usuario deberá reportar de forma inmediata a al gerente, cuando se localiza riesgo determinado real o condicional sobre equipos de cómputo, semejantes de intento de sustraer información de la ferretería Corintios.

El usuario tiene el deber de proteger las unidades de almacenamiento en su responsabilidad, en el momento que no se utilicen y contengan información confidencial.

Es responsabilidad del usuario eludir los medios extraíbles, en todo instante, así como la perdida de información que se encuentre almacenada en los equipos de cómputo asignados por la ferretería corintios.

5.3.7 Control de Acceso Físico.

El ingreso de persona externa que tenga entrada a las instalaciones de la Ferretería corintio para ceder a la red deberá chequearse al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento que no sean pertenencia de la entidad, al gerente.

Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrán ser retirados de las instalaciones, exclusivamente con el permiso de la alta gerencia de la ferretería corintios.

5.3.8 Seguridad en áreas de trabajo.

La data center de Cómputo de la ferretería corintios, es área limitado, por lo que solo el personal calificado por la gerencia puede acceder a él.

5.3.9 Protección y ubicación de los equipos.

El personal de la Ferretería Corintio no debe trasladar o mudar los equipos de cómputo, acomodar dispositivos, ni separar sellos de los mismos sin el permiso de la gerencia, en caso debe ser notificado.

El equipo de cómputo asignado deberá ser para uso único para el desempeño de los funcionarios o servidores de la ferretería.

Será compromiso del usuario requerir la capacitación indispensable para el manejo del software que se utilizan en su equipo, a fin de prevenir riesgos por mal uso y para explotar al máximo.

Durante la operación del equipo de cómputo, no se deberá comer, beber alimentos o tomar líquidos.

Se debe obviar de colocar objetos arriba de los equipos de cómputo u obstruir las salidas de ventilación del monitor o de la CPU.

Se deben proteger los equipos informáticos en lugares limpios y sin ninguna presencia de humedad.

Los usuarios deben garantizar que los cables de conexión no sean pisados al situar otros objetos arriba o contra ellos en caso de que no se satisface solicitar un traslado de cables a la gerencia.

5.3.10 Prohibido el uso de dispositivos extraíbles.

En las instalaciones de la ferretería corintios no está autorizado el de uso de artefactos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de CD y DVD Externos. Incluso están implementadas políticas de impedimento en las estaciones de trabajo.

5.3.11 Administración de Operaciones en Infraestructura de red.

Los funcionarios son responsables de proteger la información a usar en la infraestructura tecnológica de la ferretería. De igual forma, son responsables de la información reservada de la ferretería que se propaga en la red.

Los usuarios de la ferretería que hagan uso de equipos de cómputos y deseen conectar a la red, deben primero corroborar con la gerencia para después conocer y utilizar las medidas para la prevención de código dañino y Software de hurto de información.

La gerencia establecerá las políticas en su infraestructura de red para su seguridad y limitar las políticas y métodos administrativos para regular, inspeccionar y detallar el acceso de visitantes no autorizados a las instalaciones de la data center restringido o de la red.

Los funcionarios no autorizados o visitantes deben solicitar el ingresar a la red donde se encuentra conectados los Servidores y los pc que en ella trabajan, la solicitud debe ser mediante documento interno debidamente firmado y autorizado por la gerencia y se debe solicitar con anticipación para su revisión y preparación de la solicitud.

5.3.12 Seguridad de la Red.

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la el área de la gerencia, en la cual los usuarios o funcionarios realicen la exploración de los recursos informáticos en la red de la ferretería corintios, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

5.3.13 Políticas de Internet.

Las estaciones de trabajo dentro las instalaciones tienen prohibidas las conexiones al uso del internet. Exclusivamente la gerencia y administrativos están autorizados para el uso del servicio en la web.

Todos los activos fijos de la compañía deben estar con las actualizaciones requeridas y con el respaldo de un sistema de antivirus con las garantías necesarias y poder realizar las labores de monitoreo en la navegación en la web de cada estación de trabajo de la ferretería corintios.

5.3.14 Violaciones de la seguridad informática en la red.

La manipulación o instalación de herramientas de hardware o software que viole las políticas de seguridad informática establecidos en la ferretería. Automáticamente se procederá con un proceso interno para la sanción aplicada.

Los usuarios no tienen la facultad para probar o intentar probar fallas de la Seguridad Informática o de la información dentro la red de la Ferretería Corintio. Al menos que estas pruebas sean dirigidas y aceptadas por la Oficina de la gerencia.
Es obligación del usuario a quien se le asignó el equipo de escritorio o portátil velar por la buena actividad del equipo y recursos, así como la información incluida en la misma.

El traslado o reubicación del área de los usuarios, el equipo asignado a éste deberá mantenerse dentro del área nombrada originalmente.

Ningún funcionario tiene la autorización libre para realizar cambios en la red por su propia virtud como funcionario de la ferretería. Se debe realizar la consulta con la gerencia para determinar los cambios necesarios para la ejecución de la actividad. Con los controles y las buenas prácticas en el área de la seguridad de la información, se puedan mitigar las vulnerabilidades y con la implementación del sistema de detección de intrusos basado con el software Snort, donde garantizara las alertas que se generen durante el filtrado y captura del tráfico o información que circula en la red, y poder darle la administración necesaria para la ferretería corintios.

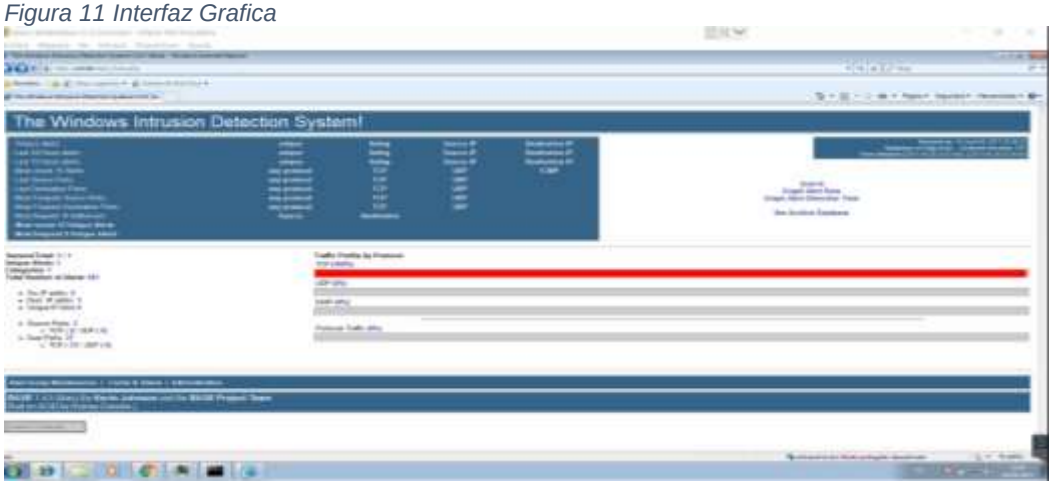
5.4 FASE IV ELABORACION DE INFORME FINAL Y RESULTADOS DE LAS PRUEBAS REALIZADAS.

5.4.1 ELABORACION DE INFORME

A continuación, se describe la interfaz gráfica con la cual se realizó las pruebas y verificación del tráfico que se genera en la red de la Ferretería C orintios. Con el apoyo de esta herramienta ya en su producción final después de su instalación, me informara de alertas potenciales, ataque o la presencia inminente del mismo.

La característica más importante que nos presenta esta herramienta es el motor de la interfaz, que es conocido como Base que en conjunto con todos los componentes instalados para el desarrollo del proyecto, nos presenta de una forma tan sencilla la exploración y administración de la consola de alertas. Como se muestra en la figura 11.

Figura 11 Interfaz Grafica

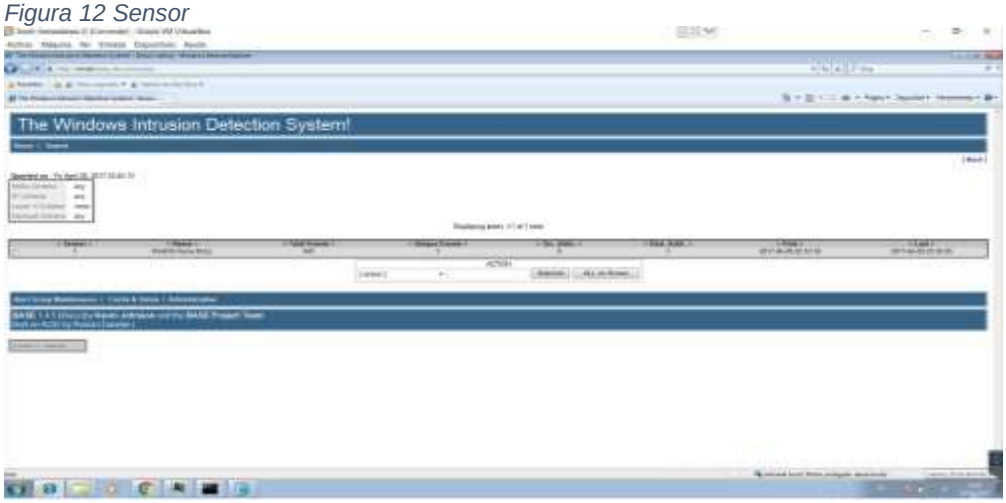


Fuente: Autor

En el momento de la prueba y la verificación en tiempo real del tráfico, se pudo verificar por medio de la herramienta de consola que el principal servicio de protocolo es el TCP, como se muestra en la anterior figura 11 en la anterior figura.

En el momento de la prueba y la verificación en tiempo real del tráfico, se pudo verificar por medio de la herramienta de consola que el principal servicio de protocolo es el TCP, como se muestra en la anterior figura 9. En la anterior figura se puede observar que la herramienta cuenta con varias opciones, en el ejercicio de las pruebas se debe escoger la que muestra en tiempo real que es el protocolo TCP y que en su momento el sensor ha detectado; con un número de 941 alertas.

Figura 12 Sensor



Fuente: Autor

En la figura 12, lo que presenta es la identificación y verificación del sensor que realiza la actividad de las alertas que se generan en el tráfico real de la red. Esta opción muestra en el momento de las pruebas que ha detectado 941 alertas.

Figura 13 Detalle de alerta detectada en protocolo TCP

Fuente: Autor

La presenta figura muestra un ataque llamado stream5: TCP sesión withous 3, el origen del ataque vine de 13 direcciones IP diferentes utilizando los puertos 80 y 443. Se observa que el sensor se encuentra realizando funciones preventivas dado que me permite detección en tiempo real.

Figura 14 Clasificación del Ataque detectado

Fuente: Autor

En la figura 14, se observa de la detección del tráfico TCP, catalogado como bad unknown, lo cual representa un aviso de presencia de paquetes anómalos

Figura 15 Detalle de la alerta detectada

Fuente: Autor

La figura 15 se observa detalladamente cada una de la IP, con sus respectivos puertos origen que realizaron el ataque host con IP 10.0.2.100. El sensor genero un solo tipo de alerta y cada uno de los ataques presentes.

Figura 16 Direcciones IP origen del Ataque

Fuente: Autor

En la figura 16, se observa claramente que fueron 10 direcciones IP, las que realizaron el tipo de ataque stream5: TCP sesión withous 3. La IP 23.229.161.2 es la que genero el mayor número de eventos de ataque. Con esta información cuenta con una herramienta que además de detectar ataques en tiempo real, también le permite implementar o combinar este mecanismo de seguridad con un firewall logrando mayor efectividad una vez es detectada la amenaza

Figura 17 Host Victima

Fuente: Autor

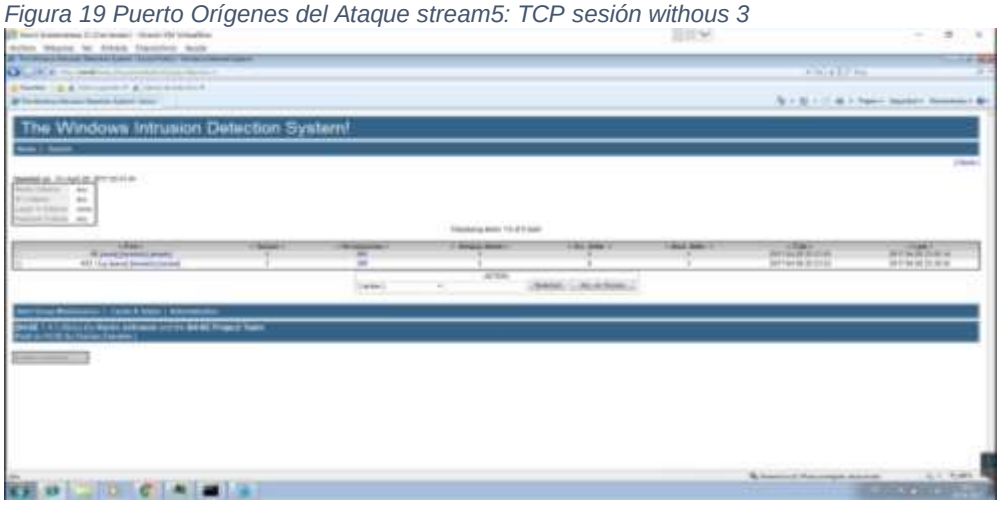
La figura 17, muestra la dirección IP destino correspondiente a la host víctima, la cual recibió ataques 958 que fueron detectados por el sensor del Snort. Se observa la efectividad de este tipo de herramientas para detectar anomalías en las cabeceras de los paquetes en la capa de red. Que a pesar de estar filtrad por firewall estarían pasando sin ningún problema.

Figura 18 Origen y Destino del ataque utilizando el protocolo TCP

Fuente: Autor

La grafica 18 se observa que el ataque utilizando el protocolo TCP, este fue generado de 10 máquinas diferentes, el sistema lo detecto y lo categorizo del tipo stream5: TCP sesión withous 3.

Figura 19 Puerto Orígenes del Ataque stream5: TCP sesión withous 3



Fuente: Autor

La figura 19, nos muestra los puertos origines utilizados para el ataque por el protocolo TCP. Estos puertos están habilitados en el firewall lo que demuestra una vulnerabilidad que fue por el sistema de detección de intrusos de Snort.

Figura 20 Puerto Destino que reciben el ataque

Fuente: Autor

La figura 20, muestra los puertos que se encuentran en la maquina víctima y que fueron objetivos del ataque. Esto quiere decir que a nivel de firewall del sistema operativo existía otra vulnerabilidad que fue aprovechada por el atacante, en la capa de seguridad a nivel de sistema operativo.

5.4.2 Recomendaciones

Para la culminación y el propósito del cuarto objetivo del proyecto es la presentación de recomendaciones que se generan del proceso de la propuesta de implementación de un sistema de detección de intrusos para la red de la Ferretería Corintio en santa marta, con base a los resultados obtenidos. Las evidencias recolectadas donde se indican son por la falta de las actualizaciones de los sistemas operativos donde se muestra la vulnerabilidad sobre el firewall del sistema operativo de las maquinas que están conectadas en la red local de la Ferretería Corintio.

Cabe anotar que estas alertas generadas por medio de la consola grafica del monitoreo es de una actividad preventiva al habilitar en el Windows Update las actualizaciones automáticas para proceder a la descarga y actualizaciones más importantes desarrolladas por la Microsoft para mantener al día nuestro sistema.

6 CONCLUSIONES

El presente proyecto es el desarrollo de una propuesta para la implementación de un sistema de detección de intrusos para la red local de la ferretería corintios en santa marta.

Para el cumplimiento de los objetivos presentados para el desarrollo del proyecto con solo propósito de ayudar a identificar los principios de la seguridad de información que son: confidencialidad, integridad y disponibilidad. Se busca es darle una guía para poder atender las fases más críticas durante el transcurso de la actividad.

En el trabajo se desarrolló una verificación del estado actual con que cuenta la ferretería corintios con respecto a su estado de infraestructura y configuración de la red. Como resultado se encuentra con una instalación física del cableado estructurado donde se pudo evidenciar las conexiones de la red LAN de los pc conectados. Con la verificación de su infraestructura se evidencia que posee un equipo físico que es un switch y cada pc con la configuración del direccionamiento IP de cada equipo conectado a la red local. Una de la deficiencia que presenta en esta parte del inicio del proyecto es la falta de inversión en tecnología de equipos; conllevando a la baja producción del valor agregado a sus labores.

Con la verificación visual del estado de infraestructura y configuración se procedió con la continuación del siguiente objetivo y cumplimiento de la misma; con un solo propósito que es la de provisionar de herramientas tecnológicas como es el sistema de detección de intrusos para determinar la problemática de gestión de inseguridad que se presenta. Con el objetivo de cumplir esta parte del proyecto se procedió con la investigación del software de detección de intrusos (Snort) y el que en el momento más se amolde a las condiciones por ser libre y gratuito, con las funcionalidades que ofrece para la capacidad de almacenamiento de bitácoras en archivos de texto y bases de datos abiertas, como lo es MySQL. De mostrando con pruebas realizadas en la red local del monitoreo y es su posible de alarmas que se pueden determinar con el apoyo de la interface web ACID.

También de la implementación exitosa del sistema de detección de intrusos en la Ferretería Corintio, lo cual permite a cualquier administrador que sea contrato a partir del proyecto puede determinar si está siendo atacada la red local y aporta información valiosa con la interface web ACID, para determinar la naturaleza de los ataques. Con todo este éxito del proyecto se determinaron los controles necesarios para tratar de minimizar las posibles vulnerabilidades que son más por la imprudencia de los mismos empleados por falta de conocimiento y falta de compromiso al ejercer el día a día sus labores. Los controles que se determinan en

el proyecto fue redactar varias políticas de seguridad, para generar un protocolo para el apoyo del administrador de sistema de la ferretería corintio donde podrá elegir la que crea más apropiado dependiendo del riesgo que exista.

Para terminar con el último objetivo propuesto en el proyecto se realiza un informe con las pruebas de la interface web ACID, verificando el tráfico y observar las alertas encontradas y generadas por el flujo de información presente en la red local, la cual es muy positivo para el análisis e importancia del funcionamiento de las reglas configuradas en el Snort. Donde se muestra evidentemente la alta severidad generada por que anteriormente no se podía determinar el origen y el alto impacto, pero luego de realizar las consultas de varias fuentes, se encontró que eran procesos normales de los protocolos de red.

Se puede concluir que Snort es un software IDS de una gran aceptación, gratuito, multiplataforma, de código abierto, actualizaciones y con su propio soporte técnico, para enfrentar y mantener al frente de las últimas amenazas. Espero que con el desarrollo del proyecto se de apoyo para futuros procesos y estudios a realizar para mitigar y ayudar de las posibles amenazas para tratar de vulnerar las defensas de las empresas en Colombia y el mundo.

7 RECOMENDACIONES

En base con los hallazgos que se realizaron a lo largo del proyecto se determinó las siguientes recomendaciones que puedan apuntar también a los objetivos planteados.

El IDS se necesita de la monitorización continua por parte del responsable la seguridad para avisar al administrador de las maquinas atacadas de la posibilidad de una intrusión en la red local y maquinas.

Hacer cumplir como orden de la gerencia a todos los empleados las políticas de seguridad planteadas en el proyecto como eje principal y tratar de generar una cultura en las labores diarias, demostrándole y educando de la importancia de la misma. Para generar la confianza de los empleados, incluir capacitaciones de los temas de seguridad, privacidad y confidencialidad de la información, e ingeniería social. Estas capacitaciones deben ser realizadas desde el inicio de la vinculación y durante la permanencia de los empleados d la ferretería, de esta manera se garantiza una mayor conciencia del manejo y aplicación de sus rutinas diarias en sus actividades laborales.

Se le solicita a la gerencia de mayor inversión en el área de comunicación donde se alojan los equipos y posibles cambios en su tecnología de equipos de cómputo, compra de una licencia de antivirus, estar pendiente de las actualizaciones generadas por parte de la Microsoft para mitigar la vulnerabilidad.

8 BIBLIOGRAFIA

ANDERSON, James. Computer security threat monitoring and surveillance. En Línea. Fort Washington, Pa. Febrero 26, 1980. 6p. Disponible en:https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf

BARNYARD2. Using Barnyard2 in Snort. Mayo 25 2017. Disponible en: https://www.honorsociety.org/articles/using-barnyard2-Snort.

BRITOS, Jose Daniel, Detección de Intrusiones en redes de datos con captura distribuida y procesamiento estadístico. Tesis de Maestría en Redes de Datos. Buenos Aires. Universidad Nacional de la Plata. 2010. 34 p. disponible en http://sedici.unlp.edu.ar/b.

CIBERSEGURIDAD. Conpes 3701. Capacidad para minimizar el nivel de riesgo, En Línea. 25 de mayo del 2017. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-6120.html.

COLOMBIA. MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Ley 1273 (5, Enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los dato.

DOTNETFX40. Microsoft .NET Framework 4. Mayo 25 2017. Disponible en: https://www.microsoft.com/es-co/download/details.aspx?id=3324.

GARZON PADILLA, Gilberzon. Propuesta para la Implementación de un Sistema de Detección de Intrusos (ids) en la Dirección General Sede Central del Instituto Nacional Pen itenciario y Carcelario Inpec “pidsinpec”. Trabajo de Grado para Optar Título de Especialista en Seguridad Informática.

GONZÁLEZ GÓMEZ, Diego. Libro Electrónico Sistemas de Detección de Intrusiones versión 1.01. Bilbao. Universidad de Deusto. 2003. 262 p. disponible en http://www.criptored.upm.es/guiateoria/gt_m481a.htm.

GONZALEZ, Gómez Diego. Sistemas de detección de intrusiones. Versión 1.01, España, Julio 2003 129 p.

LOGS. Registro de Errores (Error Log). 25 mayo 2017. Disponible en:https://httpd.apache.org/docs/2.0/es/logs.html.

IDS, En Línea. 27 de Diciembre de 2017. Disponible en: https://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos.

LOGS. Registro de Errores (Error Log). 25 mayo 2017. Disponible en: https://httpd.apache.org/docs/2.0/es/logs.html.

MÁQUINA VIRTUAL. 25 de mayo 2017 Disponible en: https://es.wikipedia.org/wiki/M%C3%A1quina_virtual.

MIRA ALFARO, Emilio José. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Proyecto Final de Carrera. Valencia – España. Universidad de Valencia. Facultad de Ingeniería. 2001. 42 p.

MYSQL DATABASE. ¿Qué es MySQL?. En Línea. 25 de mayo 2017. Disponible en: https://www.w3schools.com/php/php_mysql_intro.asp

PHP. ¿Qué es PHP?. En Línea. 25 de Mayo del 2017. Disponible en: https://www.w3schools.com/php/default.asp

REGLAS, Snort. ¿Qué es una regla de Snort?. En Línea. 17 de Diciembre del 2016. Página web disponible en: https://www.Snort.org/faq/what-is-a-Snort-rule.

SMTP, Protocolo simple de transferencia de correo. En Línea. 26 marzo 2017. Disponible en: https://www.ibm.com/support/knowledgecenter/es/ssw_i5_54/rzair/rzairemcommnd.htm

SNORT, ¿Qué es Snort?. En Línea. Marzo 30, 2016. Página web disponible en: https://www.snort.org/faq/what-is-snort

STRAWBERRY PERL. Entorno perl. Mayo 25 2017.Disponible en: http://strawberryperl.com/.

SWITCH, Conmutador (dispositivo de red). Abril 15 2017. Disponible en: https://es.wikipedia.org/wiki/Conmutador (dispositivo de red).

TCP. Protocolo de Control de Transmisión. En Línea. 25 de Mayo del 2017. Disponible en: https://es.wikipedia.org/wiki/Protocolo_de_control_de_transmisi%C3%B3n

VIRTUALBOX. Welcome to VirtualBox.org. 25 mayo 2017. Disponible en: https://www.virtualbox.org/.

WINPCAP. ¿Qué es WinPcap?. 25 de mayo 2017. Disponible en: https://www.winpcap.org/docs/docs_412/html/main.html. .

9 ANEXO

ANEXO A Carta de Aprobación del Proyecto

FERRETERIA CORINTIOS

CERTIFICA

Que el señor **HUGO ALBERTO PAYARES BECERRA**, identificado con cedula de ciudadania No. 7.604.297, labora en la empresa con el desarrollo de su Proyecto de Grado de la especializacion en Seguridad informatica de la Universidad Nacional Abierta y A Distancia (UNAD); que se llama **IMPLEMENTACION DE UN SISTEMA DE DETECCION DE INTRUSOS PARA LA RED DE LA FERRETERIA CORINTIOS EN SANTA MARTA,** desempeñandose como el ingeniero a cargo de su propia implementacion y desarrollo de la misma.

Para constancia de lo anterior se firma en Santa Marta – Magdalena a los veinte y uno (21) dias del mes de marzo del dos mil diecisiete (2017).

Cordialmente

OLGA TAMARA
Gerente General

ANEXO B Resumen Analítico Especializado - RAE

RESUMEN RAE	
TITULO	IMPLEMENTACION DE UN SISTEMA DE DETECCION DE INTRUSOS PARA LA RED DE LA FERRETERIA CORINTIOS EN SANTA MARTA
AUTORES	Payares Becerra, Hugo Alberto.
PALABRAS CLAVES	Confidencialidad, integridad, Disponibilidad, Seguridad, Redes, Sistemas, IDS, Snort, MySQL, Amenaza, Código malicioso, Malware, Troyano.
DESCRIPCION	El actual proyecto de grado para la especialización en seguridad informática de la universidad Nacional Abierta y A Distancia tiene como propósito la implementación de un sistema de detección de intrusos para la red de la ferretería corintios en santa marta y mostrar todo el proceso de instalación y administración del programa, con el fin de generar las mejoras políticas de seguridad para la información como activo principal. Ofreciendo mitigar frente a cualquier ataque o hurto de información de la compañía.
FUENTES BIBLIOGRAFICAS	http://www.winSnort.com/,https://www.Snort.org/, https://dev.mysql.com/doc/relnotes/mysql/5.7/en/news-5-7-18.html, http://windows.php.net/download/, http://www.mintic.gov.co/portal/604/w3-article-3705.html, http://www.csl.sri.com/papers/9sri/9sri.pdf,
CONTENIDOS	El presente proyecto inicia con una introducción de la importancia del crecimiento desmedido de las tecnologías y la información del tráfico en las redes de datos a nivel mundial. Con el desborde la información a medida que pasa los años, es muy importante la seguridad de la información de las compañías y a su vez la aplicación de normar o practicas seguras que conlleven a mitigar los riesgos posibles que se generen con la administración de la información. Es por eso que en este proyecto es lo que se procedió y con el aval de la gerencia de la ferretería corintios de la ciudad de santa marta quien es la empresa piloto para el desarrollo de la misma. Donde se realiza con la infraestructura de su red y posteriormente el proceso de

	instalación y administración de un sistema de detección de intrusos en la ferretería corintios de la ciudad de santa marta, para determinar los posibles ataques para mitigar con las mejores prácticas de la seguridad de la información y dar a conocer a la comunidad en general el procedimiento.
METODOLOGIA	Método Cuantitativo, donde se pretende medir la seguridad en la red de datos de la ferretería corintios. Para la presentación del proyecto se escoge como metodología de investigación, con el apoyo y soporte del análisis de referencias como un soporte para la retroalimentación de la lectura buscando la ampliación de la visión para el desarrollo del proyecto.
CONCLUSIONES	Con el propósito del proyecto es la implementación de un sistema de detección de intrusos para la red de la ferretería corintios, el cual es todo un éxito porque ayuda al administrador conocer por medio de gráficos, protocolos y a demás alertas cuando se está procediendo a un ataque a la red y el aporte a la información tan valiosa para determinar la naturaleza de los ataques. Otra de las ventajas del presente proyecto es la generación de las alertas por medio de la consola del ACID y a su vez el origen de los ataques. Con el propósito de la generación de las buenas prácticas de seguridad de la información, se ha redactado varias políticas de seguridad donde se debe apropiar dependiendo del riesgo que en el momento se esté generando en el tráfico de la red. También se procede al proceso de instalación para que los administradores puedan realizar sus respectivas instalaciones y a su vez a administración del software de Snort por medio de Windows.
RECOMENDACIONES	Aumentar las capacidades del equipo donde está corriendo la máquina virtual del Snort. Se deben realizar ajustes al Snort para mitigar el número de falsos positivos. Se recomienda mantener actualizado el sistema operativo y firmas de reglas para la detección de vulnerabilidades en el día cero.
FECHA DE REALIZACION DEL RAE	22 DE MAYO 2017