IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED INTERNA DE LA ALCALDIA DE MONTERIA USANDO SOFTWARE LIBRE

JAYNER AHMED QUINTERO HERRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION SEGURIDAD INFORMATICA
CEAD SAHAGUN
2018

IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED INTERNA DE LA ALCALDIA DE MONTERIA USANDO SOFTWARE LIBRE

JAYNER AHMED QUINTERO HERRERA

Proyecto aplicado para optar por el título de especialista en seguridad informática

Asesor de proyecto
Yina González Sanabria

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION SEGURIDAD INFORMATICA
CEAD SAHAGUN
2018

Nota de aceptación:

_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Montería, 19 de Febrero de 2018

DEDICATORIA

Este proyecto tiene una dedicatoria especial a mi esposa, por ser esa persona que me impulsa a ser mejor en mis estudios, apoyándome y motivándome a superar retos y dificultades.

AGRADECIMIENTOS

Agradecido con Dios por permitirme alcanzar este logro con paciencia, inteligencia y sabiduría.

A mi familia por apoyarme incondicionalmente en cada etapa de mis estudios.

A los docentes de la Unad, por su labor de ser grandes orientadores en todo momento.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED INTERNA DE LA ALCALDIA DE MONTERIA USANDO SOFTWARE LIBRE

INTRODUCCIÓN

En la actualidad la información y los datos se han convertido en el activo más valioso de las empresas. Por tanto las redes donde se encuentran, han sido expuestas a ataques informáticos de manera constante, de forma que ha sido necesario implementar medidas de seguridad para proteger los recursos.

Aun cuando en las empresas se han realizado acciones de prevención y protección de la información, a través de elementos de software y de hardware para prevenir ataques externos, es necesario aumentar los niveles de seguridad dado que en ocasiones se pueden presentar intrusiones o ataques internos. No se puede limitar la seguridad de la empresa a la configuración de un buen equipo de firewall, ya que este y los demás elementos de la red son víctimas de ataques e intrusiones, intrusiones que no son alertadas o verificadas en el momento que ocurren.

Resulta entonces indispensable la puesta en marcha de mecanismos de detección de intrusos, que puedan dar aviso al administrador de las redes cuando se lleven a cabo intrusiones a la red, para así tomar acciones que permitan detener ataques a la seguridad de los datos.

Es así como nace la idea de la implementación de un sistema de detección de intrusos para la red de la alcaldía de Montería con software libre, a través de la ejecución de dicho proyecto se busca minimizar el número de intrusiones en la red, previniendo ataques y daños a la información.

1. PROBLEMA

1.1 DEFINICION DEL PROBLEMA

Con el creciente uso del internet y de las tecnologías de la información, ha aumentado también el número de accesos no autorizados de intrusos a los datos e información de las empresas, convirtiéndose en uno de las problemáticas más recurrentes en la actualidad. Así mismo buscando minimizar el número de accesos no autorizados, las empresas han realizado inversiones en la adquisición de dispositivos que permitan blindar la información, como lo es el uso de firewall, con el cual se ha disminuido este tipo de ataques; pero a la vez los atacantes han perfeccionado sus métodos para lograr ingresar. Ataques como gusanos, troyanos, que atraviesan los firewalls por medio del uso de protocolos comunes, como por ejemplo el envió de archivos ocultos por correo electrónico, dejando las redes de las empresas completamente expuestas.

Ante este tipo de situaciones surge la necesidad de implementar otro tipo de herramientas, que identifiquen en el menor tiempo posible accesos no autorizados de intrusos a la red.

1.2 DESCRIPCIÓN DEL PROBLEMA

Día a día el auge y crecimiento del uso de las tecnologías de la información en las empresas y organizaciones es innegable. Ha permitido dar eficiencia y eficacia en la ejecución de procesos al interior de las mismas, se ha transformado en un eje transversal e importante para el correcto funcionamiento.
Ahora bien, gran parte de las instituciones públicas en Colombia implementan herramientas de las tecnologías de la información no solo para almacenar o procesar información, sino también para protegerla a través de la puesta en marcha de sistemas de seguridad que permitan resguardar los recursos, activos, e información, de software malicioso como los virus, malware, ataques cibernéticos, y de accesos no autorizados. Además de proteger se evita un mal funcionamiento de los procesos, perdida de información, perdida del buen nombre de la institución, y la obtención de una mayor rapidez en la ejecución de los procesos.

Una de esas entidades públicas, es la Alcaldía de Montería, la cual en la actualidad cuenta con gran infraestructura tecnológica, compuesta por hardware, software y aproximadamente 150 usuarios en la sede principal, los cuales hacen uso de equipos de cómputo, que a la vez consultan servicios tecnológicos como internet, sistemas de información, y plataformas en línea del estado, ente otros; dicha infraestructura es administrada por la oficina de sistemas, quien considera relevante que la entidad plantee acciones y mecanismos que garanticen la seguridad de la información.

Ahora bien, la Alcaldía de Montería a través de las diferentes dependencias y secretarias que la conforman, han implementado en sus procesos el uso de información digitalizada, aplicaciones informáticas, redes y sistemas de información, con información relevante de los ciudadanos. Lo que resulta en una mayor sensibilidad y tratamiento de estos, dado que no es ajena a cualquier tipo de ataques e intrusiones por parte de personas malintencionadas.

Para la Alcaldía de Montería la seguridad es de vital importancia en el correcto funcionamiento de sus redes de datos y de la información que se transmite, por lo que se debe garantizar a través de los pilares de la seguridad, la confidencialidad, integridad y disponibilidad de la información en todo momento. Previniendo que el riesgo de ataques sea reducido o el más mínimo posible, dado que en los últimos años las entidades públicas se han convertido en objetivos de los hackers o personas malintencionadas. Si se llegase a presentar una brecha de seguridad en las redes, podría ocasionar daños irremediables a la integridad de la información, dejando sin servicio a los usuarios finales, o capturando información sensible de la ciudadanía.

Es muy preocupante la vulnerabilidad en cuanto a ciberseguridad se refiere en los entes territoriales y nacionales, más aún cuando en las instituciones públicas se procesan muchos datos de la ciudadanía, información de usuarios, información de contratos y licitaciones, planes entre otros documentos de mucha relevancia.
Algunas de las amenazas a las cuales está expuesta la entidad ya sea pública o privada son: phishing, código malicioso, computadoras infectadas por bots, ataques a redes, por mencionar.

El creciente uso y estrategia de las tecnologías de la información plantea a la Alcaldía de Montería la necesidad y compromiso de mejorar las herramientas de seguridad, ya que la información que maneja la entidad debe contener el mínimo de riesgo de pérdida y mayor control en su acceso. Se plantea entonces la

oportunidad de implementar un sistema de detección de intrusos para el control de vulnerabilidades para la red interna de la Alcaldía de Montería.

1.3 FORMULACION DEL PROBLEMA

¿Cómo detectar posibles intrusos en la red interna de la alcaldía de Montería?

2. JUSTIFICACIÓN DEL PROYECTO

Gracias a los sistemas de detección de intrusos en posible contener ataques a la infraestructura tecnológica de una entidad, para el caso de la alcaldía de Montería siendo de carácter gubernamental, se siempre velar por preservar la seguridad e integridad de la información.

Los diferentes sistemas de información que utiliza la sede principal de la Alcaldía de Montería deben estar disponible todo el tiempo, dado que los sistemas son usados por los usuarios de la entidad, y se llegara a presentar una falla o intrusión, debe ser corregida de inmediato para dar continuidad a los servicios que presta la entidad.

Con la implementación de este proyecto se busca beneficiar a los empleados de la entidad, los cuales a través de los activos de información que manejan al interior de la misma, se proveen de mayor seguridad en la disponibilidad, integridad y confidencialidad de los mismos. A la vez que aumenta la confianza en el uso de las herramientas tecnológicas por parte de los usuarios, que en muchas ocasiones ven en estas un riesgo de fiabilidad en la información. También se ven beneficiados la ciudadanía en general ya que al estar protegidos los activos de información, le garantiza la confidencialidad de los datos y sus transacciones.

El beneficio en general con el desarrollo del proyecto es de gran importancia, dado que el contenido a implementar provee de un gran beneficio para la Alcaldía de Montería, pudiéndose aplicar a las sedes externas de esta entidad que deseen mejorar la seguridad en las redes y sus sistemas informáticos.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Implementar un sistema de detección de intrusos en la red interna de la Alcaldía de Montería, a través de la implementación de diversas herramientas de seguridad informática.

3.2 OBJETIVOS ESPECÍFICOS

- Detallar la situación actual de la red de datos de la Alcaldía de Montería.
- Verificar que IDS es necesario implementar en la red de datos de la Alcaldía de Montería.
- Documentar paso a paso la implementación del IDS en la red de datos de la Alcaldía de Montería.
- Efectuar pruebas que permitan verificar la eficacia del IDS en la red de datos de la Alcaldía de Montería.

4. ALCANCE Y DELIMITACION DEL PROYECTO

El desarrollo de este proyecto está dirigido a la sede principal de la Alcaldía de Montería, ubicada en la calle 27 nro. 3 – 16 de la ciudad de Montería.

Las áreas principales y con mayores riesgos a cubrir son las siguientes, Secretaria de Hacienda, Contratación, Secretaria de Salud, Recursos Humanos y Oficina de Sistemas.

En la sede principal se encuentran tres bases de datos, servidores de datos, servidores de aplicaciones y estaciones cliente, que acceden a los recursos a través de la red LAN alimentando las base de datos y accediendo a aplicaciones.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Teniendo en cuenta proyectos relacionados donde han planteado situaciones o casos similares a la problemática expuesta en este proyecto, se describe a continuación alguna de las soluciones planteadas para tenerlas como referencias.

La ingeniera Vanessa Gonzales Márquez planteo un modelo de ***Detector de Intrusos Basado en Sistema Experto*** en el Instituto Politécnico Nacional de México, en el cual se permita la toma de un equipo de cómputo que se encuentre afectado por código malicioso y aislarlo del resto de la red, para así evitar que se vea comprometida la seguridad del resto de equipos. Para la solución a este inconveniente, se utilizó la herramienta Fira, enlazada con un módulo de alertas que envía la información de las maquinas que se encuentran comprometidas, a través de una lista de direcciones ip.

En la Universidad de Valencia en España, Emilio José Mira Alfaro realizo la ***Implantación de un Sistema de Detección de Intrusos*** en la troncal de un nodo regional de universidades que tuviera un tráfico significativo. Para esto se realizó la puesta en marcha de un sistema automático que realizara la tarea del envío de correos electrónicos con un informe de las alertas de intrusiones diarias al administrador de sistemas. El administrador debía tomar la decisión de responder a la máquina que alertas debía responder a la red de origen y cuáles no. Para finalizar la maquina debía enviar las alarmas a las direcciones de correo establecidas en las instrucciones del administrador.

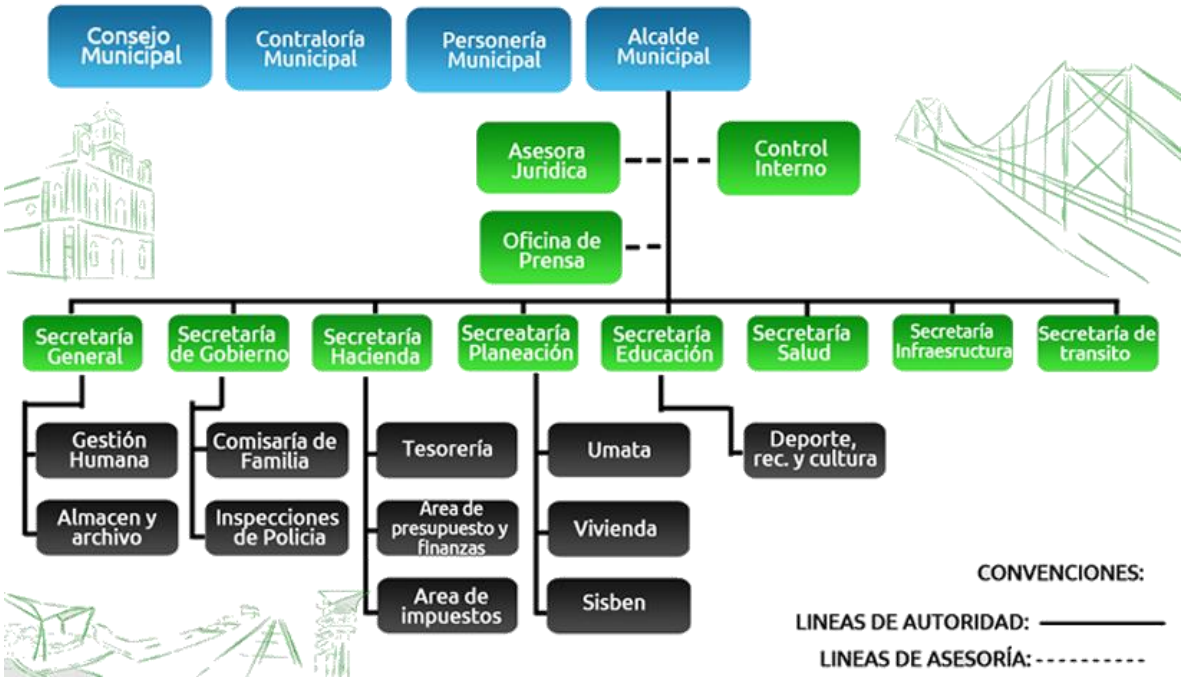
Por ultimo en la Universidad Nacional de Trujillo en Perú, se desarrolló un ***Sistema de Prevención de Intrusos para mejorar la seguridad de los servidores*** ejecutado por José Antonio Díaz Díaz y Juan Diego Salcedo Salazar, quienes a través del proyecto muestra el proceso realizado, para la correcta puesta en marcha de un sistema de detección de intrusos bajo software libre. Dicho sistema brinda la posibilidad de crear un historial y a la vez informa en tiempo real sobre posibles intrusiones o violaciones de seguridad de los servidores, por parte de usuarios no permitidos o personal malintencionadas, a través de la configuración de reglas adaptadas a las necesidades propias de la oficina de sistemas e informática de la Universidad.

5.2 MARCO CONTEXTUAL

La Alcaldía de Montería tiene como función Dirigir la Administración Municipal y representa al Municipio, sus funciones principales son la administración de los recursos propios de la municipalidad, velar por el bienestar y los intereses de sus conciudadanos y representarlos ante el Gobierno Nacional, además de impulsar políticas locales para mejorar su calidad de vida, tales como programas de salud, vivienda, educación e infraestructura vial y mantener el orden público[1].

5.2.1 Organigrama

Figura 1. Organigrama de la Alcaldía de Montería



Fuente: Tomado de http://www.monteria.gov.co/alcaldia/fundamentos/

[1] ALCALDIA DE MONTERÍA. Fundamentos [En Línea]. http://monteria.gov.co/alcaldia/fundamentos/ [citado el 04 de Octubre de 2017]

5.2.2 Misión. Gobernar a Montería de manera participativa y con enfoque social, donde el servicio público se preste con compromiso de las dependencias y sus funcionarios.[2]

5.2.3 Visión. Proyectar a Montería como la ciudad verde de Colombia, visionada como modelo de desarrollo sostenible, planificando integradamente lo urbano con el campo, garantizando el mejoramiento en la calidad de vida de los y las monterianas a través de una gestión eficiente, transparente y participativa.[3]

[2] ALCALDIA DE MONTERÍA. Fundamentos [En Línea]. http://monteria.gov.co/alcaldia/fundamentos/ [citado el 04 de Octubre de 2017]
[3] ALCALDIA DE MONTERÍA. Fundamentos [En Línea]. http://monteria.gov.co/alcaldia/fundamentos/ [citado el 04 de Octubre de 2017]

5.3 MARCO TEORICO

5.3.1 ¿Qué es seguridad?. La seguridad puede definirse como la condición de que un activo informático, información o infraestructura tecnológica esté libre de riesgos, daños o peligro.

5.3.2 Seguridad Informática. Con la seguridad informática se permiten establecer normas y medidas que tienen como objetivo proteger la información a través de las propiedades de confidencialidad, integridad y disponibilidad.

Definiendo las propiedades de la seguridad informática tendríamos:

Confidencialidad como la capacidad de acceder a la información solo por usuarios autorizados, además de forma controlada.

Integridad estaría brindada cuando al realizar modificaciones sea realizada por autorización previa.

Disponibilidad de todos los sistemas e información en todo momento, sin embargo solo debe ser accesible por autorización.

5.3.3 Seguridad en redes. La seguridad en las redes, ya sea cableada o inalámbrica a tomado mayor relevancia al interior de las empresas, protegiendo los datos e información que en ellas se transmiten. Si se llega a presentar casos de intrusiones no autorizadas a las redes, pueden llegar a causar graves daños como pérdida de información, pérdida de tiempo y de dinero, y robo de información y archivos importantes.

Durante las intrusiones se pueden presentar diferentes tipos de amenazas según la finalidad de los piratas informáticos o personas no autorizadas, la clasificación es la siguiente.

- Robo de Información
- Robo de identidad o de usuarios
- Perdida y manipulación de datos

- Interrupción del servicio

Además, dichas amenazas de seguridad, se pueden generar de forma interna o externa en las redes informáticas.

- Amenazas internas: estas amenazas son realizadas por lo general, por los mismos usuarios que laboran al interior de las empresas, y tienen cierto conocimiento para acceder a los datos e información.[4]

- Amenazas externas: son perpetradas por personas ajenas a las empresas, y son denominados hackers, que tienen altos conocimientos en programación y redes, y los utilizan para violar la seguridad y acceder a las redes para la obtención de información relevante. Logran ingresar inicialmente desde internet, o a través engaños de correos electrónicos, o lanzando ataques a los servidores de las empresas para interrumpir el servicio.[5]

Teniendo en cuentas dichas clasificaciones de amenazas y tipos de amenazas, también se han acuñado términos para describir y encasillar a las personas malintencionadas que logran intrusiones a los sistemas, dentro de los más conocidos se encuentran los siguientes.

- Hackers: son personas con gran conocimiento en programación, que buscan acceder a los recursos de las redes realizando intrusiones.
  Dentro de estos se encuentran.
  Hackers de sombrero blanco: estos atacan las vulnerabilidades de los sistemas y redes, para que luego las empresas realicen las correcciones.
  Hackers de sombrero negro: Estos buscan beneficios propios como el dinero o personal, a través de intrusiones a las redes.

- Cracker: estos hacen parte de los hackers de sombrero negro, y su particularidad es robar datos y contraseñas, además de violentar software original para distribuirlo.

---

[4] BONILLA, Sandra. GONZALEZ, Jaime. Modelo de la seguridad de la información. En: Ingenierías USBMed. Enero – Junio, 2012, vol. 3, no. 1, p. 7
[5] BONILLA, Sandra. GONZALEZ, Jaime. Modelo de la seguridad de la información. En: Ingenierías USBMed. Enero – Junio, 2012, vol. 3, no. 1, p. 7

- Phreaker: este hacker se dedica a realizar intrusiones a las telecomunicaciones, sea telefonía fija, móvil o de voz ip.

Dentro de los ataques informáticos que realizan los hackers sobre las redes, se tienen los siguientes.

- Ataques man in the middle (Mitm): en dicho ataque un equipo escucha a través de un software de monitoreo las transmisiones en la red, se hace pasar por un equipo legal de la red para capturar información.

- Ataques de denegación de servicios: consiste en dejar inactivo un servicio o servidor, a través de ataques de un equipo o red de equipos, consumiendo la banda ancha, resultando en la no disponibilidad para los usuarios legítimos.

- Ataques de replay: a través de este ataque una transmisión de red es repetida con el fin de evitar ser detectada, haciéndose pasar por la señal original enmascarando un ataque.

Ahora bien, la seguridad en la red, depende de los elementos con los que se pueda detectar, bloquear, o denegar un ataque. Con la masificación de los servicios en la red, también se han multiplicado y diversificado los ataques. Por lo tanto, la implementación de herramientas y dispositivos tanto hardware como software, se ha convertido en una necesidad de primera mano. Dentro de los más comunes se encuentran Firewall o cortafuegos, proxy.

- Firewall o cortafuegos: elemento que puede ser hardware o software o una combinación de ambos, que está diseñado para bloquear el acceso no autorizado, y a la vez tráfico permitido. Todo se reduce a los criterios de seguridad especificados o configurados.[6]

- Proxy: Es un dispositivo o software que controla y administra el acceso a internet en un red, permitiendo o negando el acceso a diferentes sitios web, evitando el entrar a ciertas paginas peligrosas.

[6] PRIMO, Álvaro. Seguridad perimetral. Cortafuegos. Enero, 2012. p. 7.

5.3.4 Seguridad Perimetral. La seguridad perimetral es una variante de la seguridad informática que tiene como objetivo vigilar el perímetro o borde de la red, utilizando un conjunto de medidas, herramientas y técnicas con el fin de neutralizar las amenazas externas que intentan filtrase a nuestra red.[7]

Esta se compone de varios elementos tecnológicos, tanto de software como de hardware, con el propósito de permitir accesos a determinados usuarios internos y externos a determinados servicios de nuestra red, realizándolo de manera oportuna protegiendo los recursos e información. Los componentes imprescindibles para establecer seguridad perimetral en la red se detallan a continuación.

5.3.4.1 Router de Frontera o de Perímetro. Dirigen el tráfico adentro, afuera de o dentro de nuestras redes. El border router es el último router que controla antes de Internet. Debido a que todo el tráfico interno va a través de este router, este funciona como el principio de una red y la última línea de defensa a través del filtro inicial y final.[8]

5.3.4.2 Cortafuegos o Firewalls. Es un dispositivo de red que se encarga de controlar los puertos y conexiones, ya sean clientes o servidores, en donde se define una política de acceso, permitiendo o denegando el tráfico según reglas previamente establecidas[9]. Dentro de su clasificación se encuentran los siguientes.

- Entrantes: es el que controla las peticiones que “entran” a nuestra red, verifica que direcciones están permitidas para poder acceder a un servicio del servidor.

- Salientes: es el que controla las peticiones que “salen” de nuestra red, verifica que direcciones están permitidas para poder brindar un determinado servicio del servidor

- Controlar el tipo de conexión: debido a que existen programas que pueden alterar el tipo de conexión de nuestro servidor con el fin de violar su

[7] PRIMO, Alvaro. Seguridad perimetral. Elementos básicos de la seguridad perimetral. Enero, 2012. p. 6
[8] CASAL, Manuel. Arquitectura de Seguridad. Fundamentos de seguridad perimetral. 2007. p. 5.
[9] PRIMO, Alvaro. Seguridad perimetral. Cortafuegos. Enero, 2012. p. 7

seguridad o simplemente dejándolo fuera de servicio, la mayoría de firewalls ya están preparados para poder rechazar posibles peticiones de programas que intentan realizar una conexión extraña.[10]

- Controla la denegación del servicio: la denegación de servicio se da cuando el servidor sobrepasa el número permitido de conexiones establecidas, logrando así saturar el servidor y que futuras conexiones no puedan acceder a sus. Para que esto no ocurra el firewall evaluara la cantidad de peticiones provenientes de una misma dirección, puede añadir reglas para bloquearlas y mantener el servicio a salvo[11].

- Controlar las aplicaciones que acceden a un puerto: el firewall nos notificara cuando una aplicación desee utilizar un puerto para esperar conexiones entrantes.[12]

- Controlar las aplicaciones que acceden a internet: cuando ya se tiene un conjunto de reglas con las conexiones más habituales y los puertos que utilizan, es posible detectar si alguna aplicación extraña desea conectarse a Internet.[13]

5.3.4.3 Ids (Sistema de detección de Intrusos). Un sistema de detección de intrusos es una aplicación es utilizada para detectar accesos no autorizados a un ordenador o servidor de nuestra red.[14]
La importancia de los IDS es fundamental para las redes ya que busca proteger de amenazas que aparecen cuando se incrementa la conectividad de la red y la dependencia que tenemos hacia los sistemas de información.

5.3.4.4 Redes Privadas Virtuales. Las redes de conexión local de una empresa permiten la conexión de los diferentes usuarios de manera particular, conforme se van expandiendo las organizaciones es necesario expandir las conexiones de red

[10] PRIMO, Alvaro. Seguridad perimetral. Otros tipos de cortafuegos. Enero, 2012. p. 9
[11] PRIMO, Alvaro. Seguridad perimetral. Otros tipos de cortafuegos. Enero, 2012. p. 10
[12] PRIMO, Alvaro. Seguridad perimetral. Otros tipos de cortafuegos. Enero, 2012. p. 10
[13] PRIMO, Alvaro. Seguridad perimetral. Otros tipos de cortafuegos. Enero, 2012. p. 11
[14] PRIMO, Alvaro. Seguridad perimetral. Sistema de detección de intrusos. Enero, 2012. p. 11

ya sea con el fin de conectar las filiales. Una solución es la de utilizar internet para realizar estas conexiones mediante un protocolo de túnel, esto significa que los datos viajaran a través de un túnel encapsulados y cifrados. Se dice que es virtual porque conecta dos redes físicas a través de internet y privada porque solo los equipos que pertenecen a una red de área local pueden ver los datos.[15]

5.3.4.5 Zona desmilitarizada. (DMZ, demilitarized zone) es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS.[16]

5.3.5 Sistema de Detección de Intrusos. Un sistema de detección de intrusos como su nombre lo indica, permite la detección de intrusos, basados en una lista de firmas o base de datos para la identificación de accesos o acciones no autorizados a un equipo de cómputo de una determinada red. El sistema actúa analizando detalladamente todo el tráfico de la red en busca de acciones como ataques conocidos, escaneo de puertos, malware, entre otros. Así también, no solo analiza el tráfico sino también revisa su contenido y su comportamiento.

Los ids se encuentran conformados principalmente por tres elementos: una fuente de información que puede ser una base de datos o firmas, un motor de análisis que se encarga de detectar las intrusiones, y un mecanismo de respuesta que actúa según los resultados que arroja el motor.

---

[15] PRIMO, Álvaro. Seguridad perimetral. Redes privadas virtuales. Enero, 2012. p. 13
[16] PRIMO, Álvaro. Seguridad perimetral. Zonas desmilitarizadas (DMZ) y subredes controladas. Enero, 2012. p. 16

5.3.5.1 Características de IDS. Un sistema de detección de intrusos debe contar con las siguientes características básicas para su correcto funcionamiento:

- Debe ser un sistema autónomo, que no requiera luego de su puesta en marcha, personal técnico que supervise su funcionamiento.
- Cuando se presenten fallas en el sistema debe tener la capacidad de sobrevivir ante dichos eventos.
- Contar con la capacidad de monitorearse así mismo, para verificar que no haya sido perturbado.
- El consumo de recursos del sistema debe ser minimizado, para evitar sobrecargar la máquina.
- Debe contar con la característica de adaptarse a los procesos del sistema ya instalado.
- Cuando se realicen cambios en el sistema generados por nuevas aplicaciones agregadas al ids, este debe ser capaz de soportar dichos cambios.
- Debe ser difícil de "engañar".

5.3.5.2 Arquitectura de un Ids. Para que un ids pueda funcionar correctamente en una red establecida detectando posibles amenazas o intrusiones, deberá estar compuesto en general por los siguientes elementos.

- **Fuente de recolección de datos:** Su propósito es conseguir de una manera eficiente todos los datos necesarios durante el proceso de detección de intrusos. Estas fuentes pueden ser un log o base de datos.
- **Reglas de contenido de datos:** Contiene los patrones para detectar anomalías de seguridad en el sistema.

- **Filtros:** Para analizar y comparar el trafico monitoreando en la red de acuerdo a las reglas de contenido de datos.

- **Detectores de eventos anormales en el tráfico de red:** Permite al ids desempeñar su función como detector de intrusos y amenazas para que posteriormente se evite algún ataque a la red.

- **Dispositivo generador de informes y alarmas:** El ids cuenta con sensores y dispositivos que le permiten avisar al administrador de la red sobre posibles

amenazas que puedan afectar el desempeño y funcionamiento de los elementos en la red.

5.3.6 Tipos de IDS. Los tipos más importantes de ids utilizados en el campo de seguridad son conocidos como ids basados en host y basados en red.

5.3.6.1 Ids basados en host. (HIDS: Host Intrusion Detection System). Los ids basados en host utilizan un sistema de detección en cada host independiente, no importando el ambiente de red en el que se encuentre el host, estará protegido, haciendo de este tipo de host el más completo de los dos.
Estos verifican diferentes procesos permitiendo identificar actividades sospechosas como intrusiones. Dicha actividad es posible, dado que a través de consultas a diferentes tipos de registros de archivos del sistema, servidores, red, cortafuegos, son verificados contra una base de datos interna de ataques conocidos.

Los sistemas de detección de intrusos basados en host de Linux y Unix hacen uso del log del sistema, el cual permite diferenciar los eventos registrados por tipo de daños. Este proporciona el registro de mensajes del sistema y del kernel. Estos ids filtran los registros, los verifican, marcan nuevamente los mensajes maliciosos con su propia clasificación de daños y los agrupa en su propio registro para que el administrador del sistema evalué su proceder.[17]

5.3.6.2 Ids basados en red. (NIDS: Network Intrusion Detection System). Por otra parte los ids basados en la red filtran los paquetes a través de un dispositivo simple antes de comenzar a enviar a host específicos.
Los sistemas de detección de intrusos basados en la red tienen una forma diferente de funcionar, estos escanean los paquetes de red al nivel de router, switch o host, revisan la información de los paquetes y registran cualquier paquete sospechoso en un archivo de registro especial con información añadida. Tomando los paquetes sospechosos, realizan una consulta con su propia base de datos de firmas de ataques a la red y les asignan un nivel de gravedad para cada paquete que se analiza. Si esos niveles de gravedad son muy altos, se envía un correo electrónico o un mensaje de advertencia a los miembros del equipo de seguridad para que estos determinen la naturaleza de la anomalía.

[17] Red Hat, Manual de seguridad. Detección de intrusos. Ids basados en host. 2005

Los ids basados en red pueden realizar monitoreo de grandes volúmenes de tráfico en la red, así mismo etiquetar transmisiones sospechosas. Debido a problemas de seguridad que presenta el protocolo TCP/IP, se ha convertido en una necesidad de primera mano, implementar este tipo de herramientas tipo escáneres, husmeadores y detección, que permita prevenir violaciones de seguridad por actividades maliciosas en la red, como las siguientes:

- Engaño de direcciones IP (IP Spoofing)
- Ataques de rechazo de servicio (DoS)
- Envenenamiento de caché arp
- Corrupción de nombres DNS
- Ataques de hombre en el medio

Los ids basados en red, necesitan que la conexión de red del sistema donde se encuentra configurado el sistema, se configure de modo que permita escuchar la red en ambos sentidos, permitiendo la captura de todos los paquetes que trafican por la red.[18]

5.3.7 Fortalezas de IDS

- Brinda información relevante sobre el tráfico malicioso de la red.
- La reacción para prevenir el daño es más eficaz.
- Ayuda a identificar el origen de los ataques que se producen.
- Permite identificar a través de evidencias los intrusos.
- Es una "cámara" de seguridad y una "alarma" contra ladrones.
- Lanza alertas al personal de seguridad cuando alguien intenta entrar.
- Provee un grado de tranquilidad a los administradores.
- Es un componente indispensable de la infraestructura para la estrategia global de defensa.
- Cuando se detectan ataques no conocidos, crece la posibilidad de detectar automáticamente nuevos ataques.
- No dependen de los procesos específicos de casa sistemas operativos.
- El costo de implementación y mantenimiento es bajo al ser utilizado en puntos estratégicos de la red.

---

[18] Red Hat, Manual de seguridad. Detección de intrusos. Ids basados en la red. 2005.

- No le permite fácilmente al intruso borrar sus huellas al realizar intrusiones.

5.3.8 Debilidades de IDS

- La mayoría de bugs de seguridad no cuentan con parches.
- En ocasiones pueden producirse falsas alarmas.
- Las alarmas lanzadas presentan fallas.
- Siempre será necesario un Firewall, y deberá ir acompañado de auditorías de seguridad y una correcta política de seguridad.

5.3.9 Ids Comerciales

5.3.9.1 NetRanger - Cisco Systems. El sistema de detección de intrusos de Cisco, conocido formalmente por Cisco NetRanger, 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.[19]

5.3.9.2 Dragon - Enterasys Networks. El IDS de Enterasys Networks, Dragon, toma información sobre las actividades sospechosas de un sensor llamado Dragon Sensor y de un módulo identificado como DragonSquire que es el encargado de monitorizar los logs de los firewalls y otros sistemas. Esta información es enviada a

[19] BECERRA, Armando. Sistemas detección de intrusos. Trabajo de grado Ingeniero Informático. Universidad Francisco de Paula Santander. Facultad de Ingeniería. 160 p.

un producto llamado Dragon Server para futuros análisis y correlaciones. Cada componente tiene algunas ventajas que compensan con debilidades de otro, un ejemplo seria que el sensor Dragon Sensor es incapaz de interpretar tráfico codificado de una sesión web SSL, pero el producto DragonSquire es capaz de recocer los logs del servidor web y pasárselos a la máquina de análisis.[20]

5.3.9.3 Internet Security Systems – RealSecure. RealSecure proporciona detección, prevención y respuestas a ataques y abusos originados en cualquier punto de la red. Entre las respuestas automáticas a actividades no autorizadas se incluyen el almacenar los eventos en una base de datos, bloquear una conexión, enviar un mail, suspender o deshabilitar una cuenta en un host o crear una alerta definida por el usuario. El sensor de red rápidamente se ajusta a diferentes necesidades de red, incluyendo alertas específicas por usuario, sintonización de firmas de ataques y creación de firmas definidas por el usuario. Las firmas son actualizables automáticamente mediante la aplicación X-Press Update. El sensor de red puede ser actualizado de una versión a otra posterior sin problema, asegurando así la última versión del producto.[21]

5.3.10 IDS OPENSOURCE

5.3.10.1 Suricata. Es un motor de detección de amenaza de red gratuita, madura, sólida y de código abierto. El motor Suricata es capaz de detección de intrusión en tiempo real (IDS), prevención de intrusiones en línea (IPS), monitoreo de seguridad de red (NSM) y procesamiento de pcap sin conexión.

Suricata inspecciona el tráfico de la red utilizando reglas potentes y extensas y lenguaje de firma, y tiene un poderoso soporte de secuencias de comandos Lua para la detección de amenazas complejas.

---

[20] MIRA ALFARO, Emilio José. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Proyecto Final de Carrera Ingeniero Informático. Valencia. Facultad de Ingeniería. 142 p.

[21] MIRA ALFARO, Emilio José. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Proyecto Final de Carrera Ingeniero Informático. Valencia. Facultad de Ingeniería. 142 p.

Con formatos de entrada y salida estándar como las integraciones YAML y JSON con herramientas como los SIEM existentes, Splunk, Logstash / Elasticsearch, Kibana y otras bases de datos se vuelven fáciles.

El desarrollo impulsado por la comunidad de ritmo rápido de Suricata se centra en la seguridad, la usabilidad y la eficiencia.
El proyecto y el código de Suricata es propiedad y está respaldado por Open Information Security Foundation (OISF), una fundación sin fines de lucro comprometida con asegurar el desarrollo de Suricata y el éxito sostenido como un proyecto de código abierto.[22]

5.3.10.2 Bro-IDS. Bro es un poco diferente que Snort y Suricata. En cierto modo, Bro es una firma y un IDS basado en anomalías. Su motor de análisis convertirá el tráfico capturado en una serie de eventos. Un evento podría ser un inicio de sesión de usuario a FTP, una conexión a un sitio web o prácticamente cualquier cosa. El poder del sistema es lo que viene después del motor de eventos y ese es el intérprete de Policy Script. Este motor de políticas tiene su propio lenguaje (Bro-Script) y puede realizar algunas tareas muy potentes y versátiles.[23]

5.3.10.3 Ossec. Es un Sistema de Detección de Intrusión basado en host, de codigo abierto, escalable y multiplataforma (HIDS). Tiene un poderoso motor de correlación y análisis, integra análisis de registro, verificación de integridad de archivos, monitoreo de registro de Windows, aplicación de políticas centralizada, detección de rootkits, alertas en tiempo real y respuesta activa. Se ejecuta en la mayoría de los sistemas operativos, incluidos Linux, OpenBSD, FreeBSD, MacOS, Solaris y Windows.
Cuando suceden los ataques, OSSEC le informa a través de los registros de alerta y las alertas por correo electrónico que se le envían a usted y a su personal de TI para que pueda realizar acciones rápidas. OSSEC también exporta alertas a cualquier sistema SIEM a través de syslog para que pueda obtener análisis e información en tiempo real sobre los eventos de seguridad de su sistema.[24]

---

[22] SURICATA. [En linea]. https://suricata-ids.org/ [Citado el 7 de noviembre de 2017]
[23] Open Source Intrusion Detection Tools. [En linea] <https://www.alienvault.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview>. [Citado el 7 de noviembre de 2017]
[24] OSSEC. [En linea] <https://ossec.github.io/index.html>. [Citado el 7 de noviembre de 2017]

5.4 MARCO CONCEPTUAL

Algunos de los aspectos para tener en cuenta dentro del marco conceptual que se va a manejar en el siguiente proyecto está relacionado directamente con algunos conceptos que derivan de la seguridad informática y de la información, sobre ciertas vulnerabilidades que se pueden presentar en los sistemas informáticos y que pueden afectar de gran manera el correcto funcionamiento de cada uno de los procesos que se realizan en una organización. Por eso es importante reconocer la conceptualización de los siguientes componentes.

5.4.1 Ataque cibernético. Es la acción propia de organizar métodos y formas para procurar afectar un sistema de informático, ya sea una red de datos o un equipo de cómputo en una organización o persona en particular. En los ataques informáticos lo que se busca inicialmente es una vulnerabilidad o falla en la seguridad que tenga la infraestructura informática la cual se pretende atacar, con lo que se pretende afectar ya sea el software o incluso el hardware, todas esta acciones inciden de forma negativa en los activos de una organización quienes suelen ser los blancos preferidos de las personas que realizan los ataques.

Un ataque puede ser organizados por una varias personas y a estos se les conoce como Hackers (piratas informáticos), los cuales sustentan sus acciones en ideologías sociales y económicas, pero en algunos casos solo lo hacen por diversión.
Los ataques informáticos generan consecuencias negativas en los sistemas operativos los cuales son infectados con virus informáticos, los cuales pueden variar de forma significativa el funcionamiento correcto de los activos informáticos, estos daños se pueden clasificar de la siguiente forma.

5.4.2 Daños triviales. En este tipo de daños los VIRUS que los causan son muy fáciles de remover y eliminar, por lo que se pueden quitar solo en segundos o minutos.[25]

[25] ECURED. Ataque informático. [En linea] <https://www.ecured.cu/Ataque_inform%C3%A1tico> [Citado el 7 de noviembre de 2017]

5.4.3 Daños menores. En este son virus que tienen un virus de un grado de afectación mayor, pues en algunos casos afecta el funcionamiento de programas los cuales es necesarios instalarlos de nuevo.
En este tipo de daños se tiene que tener en cuenta el virus Jerusalén. Este virus los viernes 13, borra todos los programas que una trate de usar después de que el virus haya infectado la memoria. Lo peor que puede suceder es volver a instalar los programas ya borrados por el ataque que te metió el ordenador.

5.4.4 Daños moderados. Este daño sucede cuando un virus formatea el DISCO DURO, y mezcla los componentes del FAT (File Allocation Table por su sigla en inglés o Tabla de Ubicación de Archivos por sus siglas en español, TUA), o también puede que sobrescribe el disco duro. Sabiendo esto se puede reinstalar el sistema operativo y usar el último backup.[26]

5.4.5 Daños mayores. Algunos VIRUS pueden pasar desapercibidos y pueden lograr que ni utilizando el backup se pueda llegar a los archivos. Un ejemplo es el virus Dark Avanger que infecta los archivos acumulando. Cuando llega a 16, el virus escoge un sector del disco duro al azar y en ella escribe: "Eddie lives... somewhere in time (Eddie vive... en algún lugar del tiempo) Cuando el usuario se percata de la existencia del virus ya será demasiado tarde pues los archivos más recientes están infectados con el virus.[27]

5.4.6 Daños severos. Los daños severos son hechos cuando los VIRUS hacen cambios mínimos y progresivos. El usuario no sabe cuándo los datos son correctos o han cambiado, pues no se ve fácilmente, como en el caso del VIRUS Dark Avanger. También hay casos de virus que infectan aplicaciones que al ser descontaminadas estas aplicaciones pueden presentar problemas o perder funcionalidad.[28]

---

[26] Seguridad informática. Tipos de ataques informáticos. [En línea] <http://securityinformat.blogspot.com.co/> [Citado el 7 de noviembre de 2017]
[27] ECURED. Ataque informático. [En línea] <https://www.ecured.cu/Ataque_inform%C3%A1tico> [Citado el 7 de noviembre de 2017]
[28] ECURED. Ataque informático. [En línea] <https://www.ecured.cu/Ataque_inform%C3%A1tico> [Citado el 7 de noviembre de 2017]

5.4.7 Daños ilimitados. Algunos programas como CHEEBA, VACSINA.44.LOGIN y GP1 entre otros, obtienen la clave del administrador del sistema. En el caso de CHEEBAS, crea un nuevo usuario con el privilegio máximo poniendo el nombre del usuario y la clave. El daño lo causa la tercera persona, que ingresa al sistema y podría hacer lo que quisiera.[29]

Hay diversos tipos de ataques informáticos. Algunos son:

5.4.8 Ataque de denegación de servicio. También llamado ataque DoS (Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legales, normalmente provocando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.[30]

5.4.9 Man in the middle. Es un ataque en el que el hacker, adquiere la capacidad de leer, insertar, y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas.[31]

5.4.10 Ataques de REPLAY. Una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o retardada. Es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado.[32]

---

[29] ECURED. Ataque informático. [En línea] <https://www.ecured.cu/Ataque_inform%C3%A1tico> [Citado el 7 de noviembre de 2017]

[30] Libro Curso de Ciberseguridad y Hacking Etico, Pag. 52

[31] LARIOS ESCAMILLA, Jorge. SANCHEZ GONZALEZ, Rodrigo. Ciberdelito, Ingeniero en Telecomunicaciones. Trabajo de Grado. México, D.F.: Universidad Nacional Autónoma de México. Facultad de Ingeniería. 2014. 154p.

[32] Ataques informáticos. [En línea]. https://sites.google.com/site/sykrayolab/ataques-informaticos [Citado el 7 de noviembre de 2017]

5.4.11 Ataque de día cero. Ataque realizado contra un ordenador, a partir del cual se explotan ciertas vulnerabilidades, o agujeros de seguridad de algún programa o programas antes de que se conozcan las mismas, o que, una vez publicada la existencia de la vulnerabilidad, se realice el ataque antes de la publicación del parche que la solvente.[33]

5.5 MARCO LEGAL

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del 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”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

---

[33] Ataques informáticos. [En línea]. <https://sites.google.com/site/sykrayolab/ataques-informaticos> [Citado el 7 de noviembre de 2017]

6. MARCO METODOLÓGICO

6.1 METODOLOGÍA DE INVESTIGACIÓN

Teniendo en cuenta cada uno de los aspectos anteriormente descritos el tipo de investigación que se hará uso en este trabajo de investigación será empírica, ya que se plantea una hipótesis, la cual debe ser validada a través de un trabajo práctico el cual se documentará. Así que se desarrollará una labor técnica y práctica, para llevar a cabalidad los objetivos que se pretenden alcanzar en este proyecto, la metodología empírica se basa en el experimento y la realización directa de las acciones, estas pretenden validar hipótesis planteadas. Para lograr la implementación de un sistema de detección de intrusos se requieren tanto acciones técnicas como teóricas, estas se deben converger, en la práctica y experimentación, la cual arrojará información y resultados que servirán para validar y dar soporte a la implementación de un sistema de información en la red interna de la alcaldía.

6.2 METODOLOGÍA DE DESARROLLO

Para el desarrollo del presente proyecto se deben tener en cuenta múltiples parámetros que influencian de forma directa en el funcionamiento y acciones que se realizan al interior de la entidad, la cual tienen aspectos específicos para procesamiento de la información, la cual debe ser salvaguardada en algunos casos y en otros hacerse pública cumpliendo un número de características particulares, permitiendo la mejora al interior de los procesos.

Por lo que para el desarrollo del proyecto se utilizó la metodología PHVA (Planear, Hacer, Verificar y Actuar), la cual plantea la mejora continua, para este caso en el modelo para la implementación de la herramienta de detección de intrusos a través de sus ciclos.

Planear

En este primer ciclo se determinaron todas las actividades del proyecto, la delimitación del proyecto, los recursos necesarios, el tiempo necesario para la correcta ejecución de las actividades, definición de objetivos, así mismo la

identificación de un marco contextual, antecedentes de proyecto y un marco teórico. Para esta fase inicial del proyecto se llevaron a cabo las actividades listadas a continuación.

- Análisis de información de proyectos relacionados
- Identificación del estado actual de la red de la alcaldía de Montería.
- Análisis de las herramientas disponibles para la ejecución del proyecto
- Cronograma de actividades

Hacer

Para este ciclo de la metodología se llevaron a cabo las actividades del Hacer que permitieron ejecutar los objetivos del proyecto, al igual que el producto a entregar, y el modelo de implementación de un sistema de detección de intrusos en la red interna de la alcaldía de montería usando software libre, para lo cual se ejecutaron las siguientes actividades en Fase Hacer del ciclo PHVA:

- Verificación de las características y especificaciones del servidor o equipo de cómputo donde se realizó la instalación del sistema operativo.
- Análisis de las zonas o esquemas en las que es posible realizar la instalación del sistema detección de intrusos.
- Instalación de las librerías necesarias para el correcto funcionamiento del sistema de detección de intrusos.
- Instalación y configuración del motor de base de datos para el almacenamiento de las alertas del sistema de detección, así como el lenguaje Php, y el servidor de aplicaciones apache.
- Instalación y configuración del sistema de detección de intrusos con la herramienta Snort, además de la herramienta barnyard.

Verificar

En esta tercera fase se efectuaron las revisiones y seguimiento al desarrollo del proyecto, permitiendo verificar que cada una de las herramientas seleccionadas funcionara correctamente y así dar cumplimiento a los objetivos. Así mismo se realizaron los ajustes requeridos en el documento. Para esta fase se llevaron a cabo las siguientes actividades de la fase verificar, teniendo en cuenta el cronograma de actividades.

- Revisión de cada una de las herramientas y aplicaciones, realizando pruebas que permitieron verificar su correcto funcionamiento.
- Ajustes requeridos en el documento del proyecto verificando su alineación con los objetivos del proyecto.

Actuar

Para la fase actuar de dicha metodología, se obtuvo como resultado la mejora continua de los dispositivos de red de la oficina de sistemas, a través de la implementación de un sistema de detección de intrusos en la red de la Alcaldía de Montería.

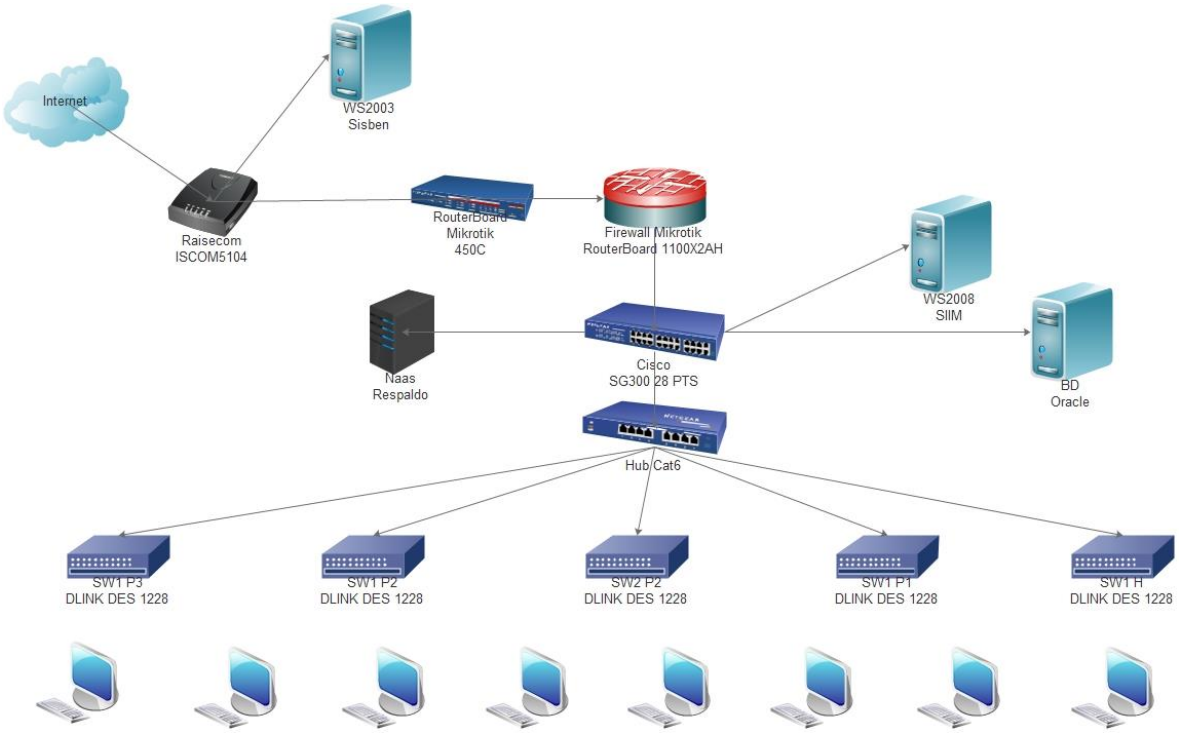
7. DESARROLLO DEL PROYECTO

7.1 DISEÑO RED ACTUAL DE LA ALCALDÍA DE MONTERÍA

La sede principal de la Alcaldía de Montería cuenta actualmente en su infraestructura con servidores de respaldo de datos, servidores de aplicaciones, estaciones cliente que se conectan a los servidores locales, así como también servidores de bases de datos, en donde se administran y almacenan datos de gran relevancia.

La siguiente figura muestra con mayor exactitud el estado de la red, con los dispositivos que la componen.

Figura 2. Red sede principal



Fuente: El Autor

Los dispositivos que componen la red, se encuentran resguardados en un cuarto de máquina, que les provee de seguridad física, además que se encuentran bajo

refrigeración para evitar su calentamiento, cuenta también con un sistema de alimentación eléctrica de 15kva que brinda suministro de energía, en casos de fallos en la alimentación externa. A continuación se describen los equipos mostrados en la figura anterior.

- Firewall Mikrotik 1100X2AH
  Dispositivo utilizado en el bloqueo de puertos, redirección de servicios, denegación de servicios, bloqueo de conexiones, asi como publicación de servicios a la web.

- Naas Lenovo Px 300
  Almacenamiento en red de 4Tb, utilizado para el respaldo de información en diferentes oficinas.

- Naas Segate
  Almacenamiento en red de 4Tb, utilizado para el respaldo de información en diferentes oficinas.

- Hp Proliant ML150 G3
  Servidor de aplicaciones web, que cuenta con sistema operativo windows server 2008.

- Hp Proliant ML150 G6
  Servidor de aplicaciones web con sistema operativo Centos 7, con servidor apache y base de datos mysql.

- Switch Cisco SG300
  Switch que interconecta los dispositivos externos, así como conecta los equipos internos de la lan, como otros switches, y distribuye conexiones a los servidores.

- Hub
  Dispositivo que interconecta los switches dlink de la infraestructura.

- Switch Dlink Des 1228 (5)
  Equipos de red que conectan los equipos de cómputo de todas las oficinas.

7.2 VERIFICACIÓN DE IDS A IMPLEMENTAR

Los sistemas de detección de intrusos son programas que escanean la actividad del sistema o de la red, con el objetivo de detectar accesos o acciones no autorizados a una máquina o a una red.

A la hora de implementar un sistema de detección de intrusos se deben tener en cuenta cuál de los dos tipos, Hids (host) o Nids (red) se desarrollara. La opción de optar por la implementación de unas estas, reside en el objetivo de que se quiere monitorear o analizar; en este caso escanear la red de la alcaldía de Montería en búsqueda de intrusiones.

Existen diferentes tipos de herramientas ids de tipo software en el mercado para la configuración y puesta en marcha, dentro del tipo Hids se encuentra Ossec y del lado de Nids, Snort.

7.2.1 Ossec. Este sistema de detección de intrusos es del tipo host, es decir analiza todo lo referente a los eventos y registros del sistema operativo del equipo donde se encuentra instalado, además comprueba la integridad del mismo, y realiza auditorias de los registros de equipos con Windows.

Además es una aplicación de código abierto y gratuito para su implementación, cuenta con amplia gama de opciones en su configuración, lo que le convierte en un software adaptable a las necesidades de seguridad; permite la personalización de reglas de alertas, así como también la definición de reglas de acción en respuesta a las alertas de seguridad anteriormente establecidas.

Dicho sistema se encuentra comprendido por tres componentes, una aplicación principal, un agente de Windows, y una interfaz web. La aplicación principal, es utilizada en redes distribuidas, donde puede soportar varios sistemas operativos como Linux, Bsd, y Mac.

El agente Windows, es utilizado en entornos Windows, configurando la aplicación principal en el modo servidor, y verificando el soporte para el agente en Windows.

Por último la interfaz web permite la visualización grafica de las alertas y funcionamiento al usuario administrador.

7.2.2 Snort. Sistema de detección de intrusos del tipo NIDS (escanea la red a diferencia de ossec, que tiene un comportamiento a nivel de equipo) por lo tanto trabaja escaneando y analizando los paquetes que circulan en la red, identifica posibles ataques según el comportamiento de estos. La manera más básica de instalar snort permite la activación de logs de sistema, guardando esos logs en una base de datos y visualizarlos desde algún administrador web.
Cuenta con licencia GPL, es gratuito y funciona bajo plataformas Linux y Windows, además que posee gran cantidad de plugins desarrollado por organizaciones independientes, convirtiéndolo en uno de los sistemas de detección más usado, así como también la integración de aplicaciones que permiten gran adaptabilidad a las necesidades de los usuarios.
En su estructura está definido por un decodificador de paquetes, preprocesadores, motor de detección, sistema de alarmas e informes.
Decodificador de paquetes es en el encargado de capturar los paquetes.
El preprocesador realiza análisis de los paquetes que han pasado por el decodificador.
El motor de detección detecta si un paquete capturado contiene algún patrón de ataque, basándose en las firmas de snort.
Por último el sistema de alarmas e informe, permite definir el que y como se guardan las alarmas generadas.

Así mismo, el hecho de ser una aplicación Open Source, Snort cuenta con la ventaja de ser un sistema configurable y adaptable a necesidades concretas, por lo que puede ser una buena solución si se busca un sistema personalizado para el desarrollo del proyecto. Este es uno de los motivos por los que se ha decidido seleccionar como un sistema de detección de intrusos utilizando Snort en lugar de otras aplicaciones, que en muchos casos no alcanzan el mismo rendimiento ni las prestaciones de esta.

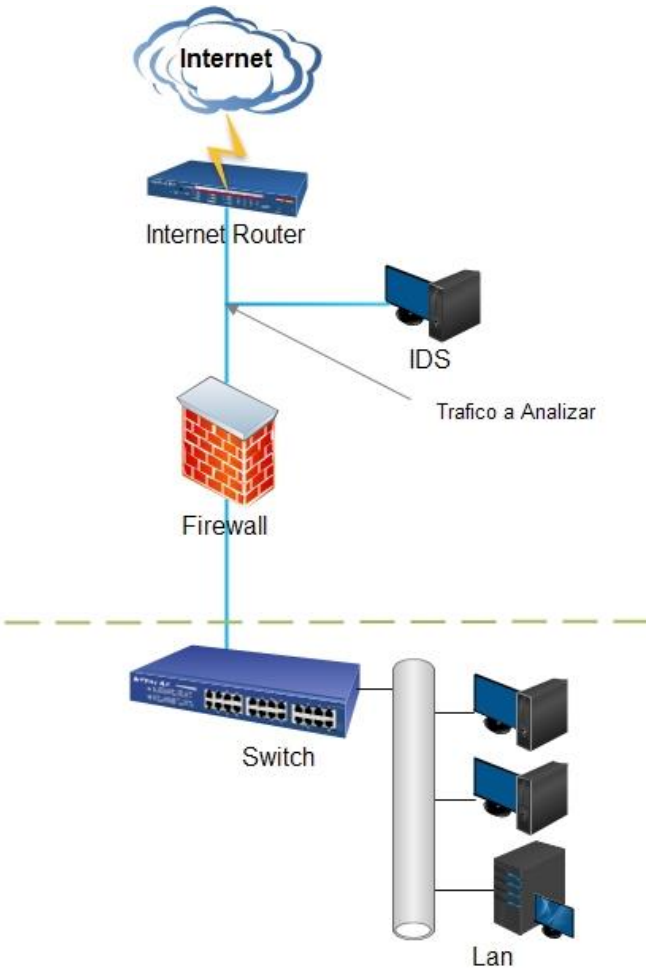
7.3 DONDE INSTALAR EL IDS

Previo a la instalación de la herramienta seleccionada Snort, se debe verificar las posibilidades donde se pueda ubicar el sistema de detección de intrusos. Para dicha ubicación se debe tener en cuenta el tráfico a escanear o detectar, paquetes entrantes o salientes, delante del firewall o detrás de este.

Sea donde fuere donde se ubique el ids, se debe garantizar su funcionamiento en conjunto con los demás elementos de la red, capturando y compartiendo información de los switches, routers y firewalls.
Es así como se muestra a continuación las ubicaciones donde se puede instalar el ids.

7.3.1 Delante del Firewall

Figura 3: Ids delante del Firewall

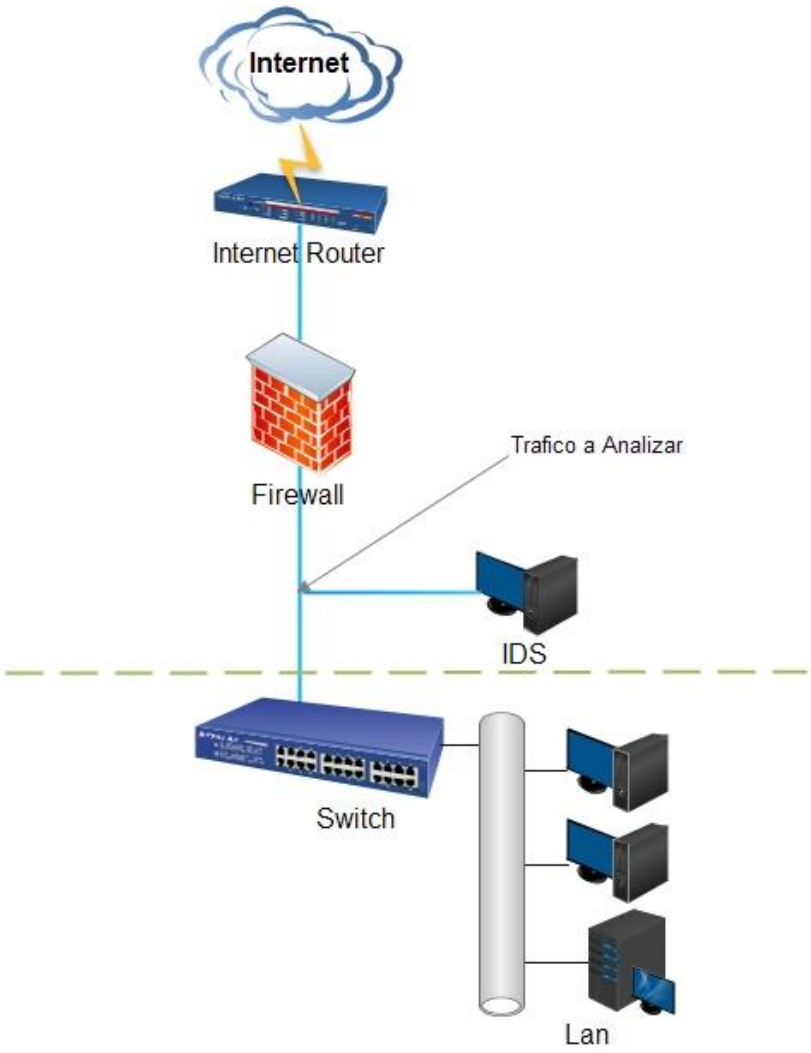


Fuente: El Autor

Con esta ubicación se generan muchos falsos positivos de ataques, además de la gran cantidad de información que se guarda en los logs, por lo que analiza todo el tráfico que entra y sale de la red.

7.3.2 Detrás del Firewall

Figura 4: Ids detrás del Firewall

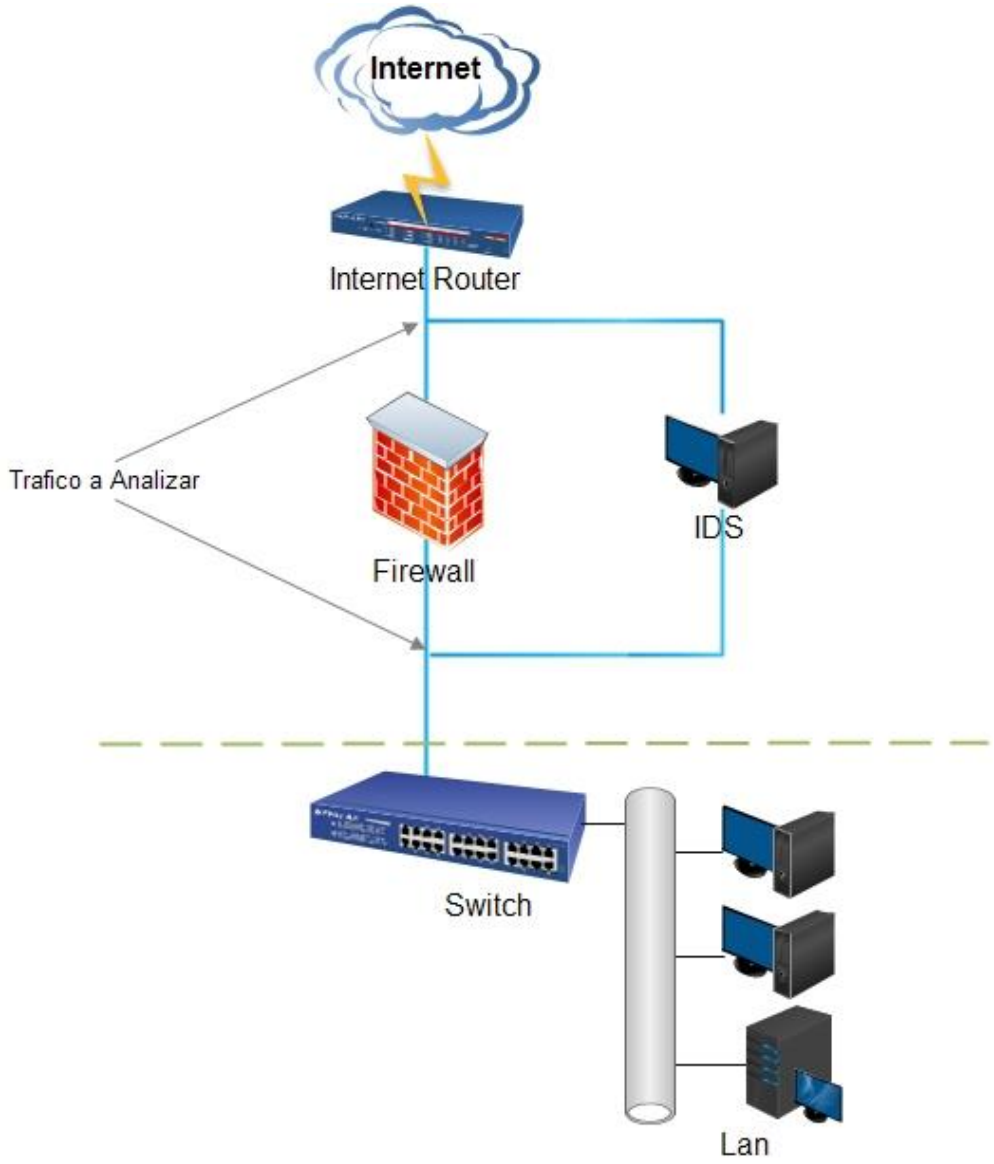


Fuente: El Autor

Configurando el ids detrás del firewall es la ubicación más utilizada, debido a que analiza el tráfico que pasa por el firewall, convirtiéndose en otro filtro para la red. Aquí se escanea el trafico realmente que ingresa a la red y que no pudo bloquear el firewall, por lo que se producen menos casos de falsas alarmas que en la ubicación anterior.

7.3.3 Combinación de los dos casos

Figura 5: Ids Combinado



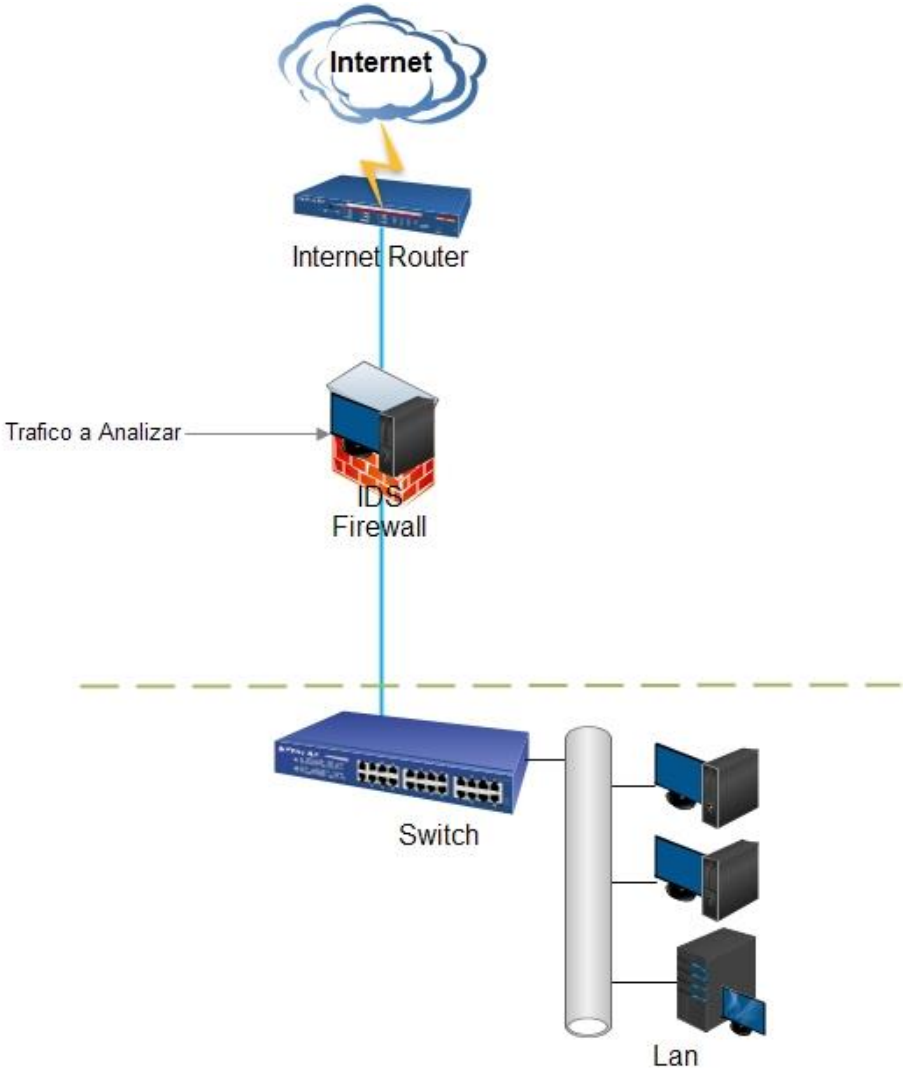
Fuente: El Autor

Configurando el ids delante del firewall y detrás del firewall se tiene un mayor control de los ataques que realmente cruzan el firewall, teniendo la oportunidad de

detectarlos si llegan a ocurrir. Dicho modelo presenta una dificultad, y es que necesita dos equipos para ponerlo en marcha.

7.3.4 Firewall/NIDS

Figura 6: Firewall/Nids



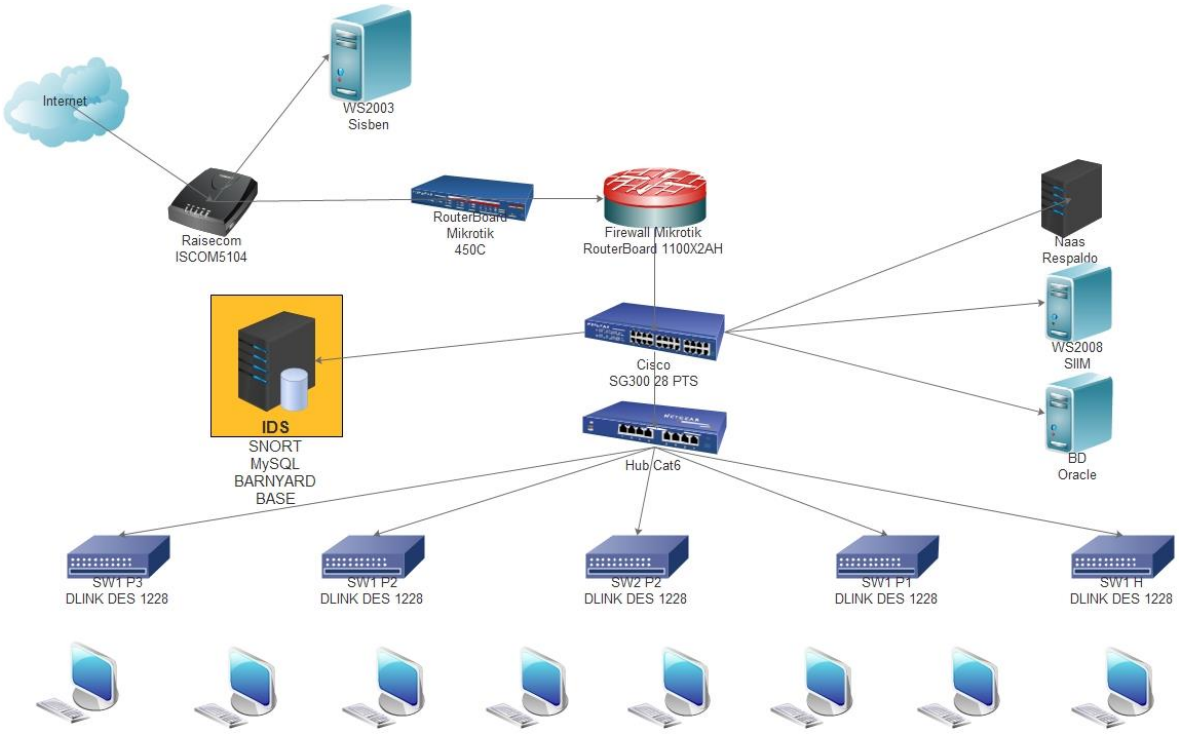
Fuente: El Autor

Con esta ubicación el objetivo es que un solo equipo realice la tarea de firewall y a la vez de ids. Realizando dicha configuración se requiere de un equipo robusto y que suele ser una solución costosa.

7.4 DISEÑO DE DIAGRAMA DE RED CON IDS

Una vez verificadas las diferentes posibilidades de instalar un ids en la red, se realiza un diagrama que permite identificar la ubicación del sistema en la red interna de la Alcaldía de Montería.

Figura 7. Diagrama de red con Ids



Fuente. El Autor

Dentro de las opciones analizadas anteriormente, se seleccionó la configuración del Ids detrás del Firewall. Además de ser otro filtro detrás del firewall, se presenta también como la configuración en donde todas las alertas que se generen serán hostiles o de mayor importancia, dado a que ha superado la primera barrera

(firewall), por lo que se traduce en menor número de falsas alarmas para el sistema. Además también resulta en la configuración menos costosa para su implementación, dado que solo se requiere de un equipo servidor a diferencia de las otras posibilidades.

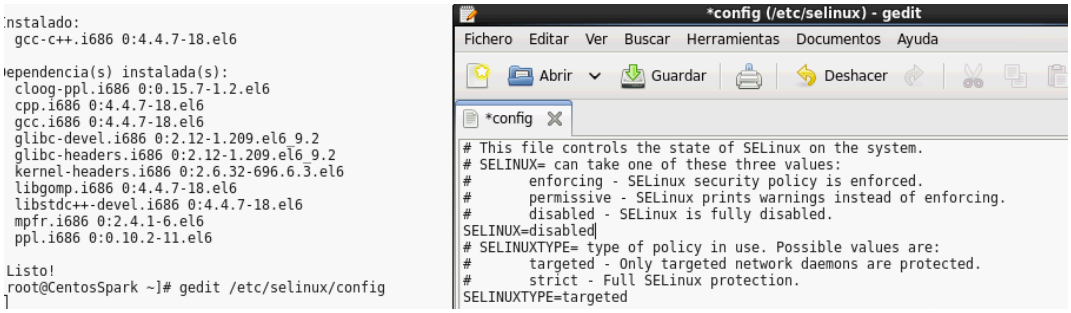
7.5 IMPLEMENTACIÓN DEL IDS EN LA RED DE DATOS DE LA ALCALDÍA DE MONTERÍA

Para instalar Snort, es necesario deshabilitar el módulo de seguridad de Linux, para que este no bloque algún tipo de instalación o configuración. Para esto, se modifica el fichero config ubicado en la ruta /etc/selinux/config y realizando los siguientes cambios, habilitando las siguientes líneas en el archivo.

#gedit /etc/selinux/config
SELINUX=disabled
SELINUXTYPE=targeted

Como se aprecia en la siguiente figura

Figura 8. Desactivando Selinux



Fuente. El Autor

Asi mismo es necesario desactivar el firewall iptables ejecutando en la terminal el siguiente comando, seguido se guardan los cambios.

#iptables –F

Posteriormente se guarda la configuración con:

iptables-save >/etc/sysconfig/iptables

También es necesaria la instalación de Libcap, la cual es una librería de programación de paquetes de TCP/IP .
Inicialmente se descarga el paquete libpcap-1.8.1.tar.gz la web www.tcpdump.org
Luego de descargado se descomprime y se compila ejecutando los comandos en terminal que se muestran a continuación.

#tar xvfz libpcap-1.8.1.tar.gz
#cd libpcap-1.8.1
#./configure
#make
#make install

Snort utiliza expresiones regulares para sus reglas por lo que es necesario instalar la librería Pcre que realiza dicha función.

Se descarga el paquete pcre-8.41.tar.gz de la página web (www.pcre.org)

Se descomprime el paquete: tar xvfz pcre-8.41.tar.gz.

Finalmente se compila y se instala ejecutando los comandos:

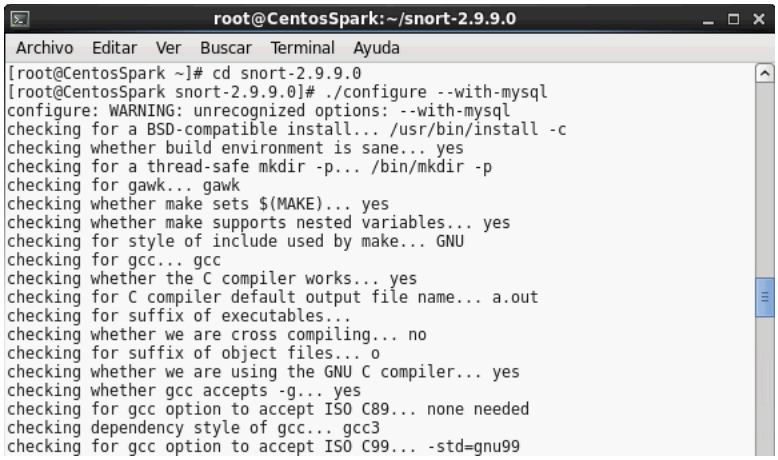
#cd pcre-8.41
#./configure
#make
#make install

7.5.1 Instalación de Snort. Para dar inicio a la instalación de snort, se procede inicialmente a descargar el paquete snort-2.9.9.0.tar.gz de la web (www.snort.org), seguidamente se descomprime con el comando tar xvfz snort-2.9.9.0.tar.gz
Para finalizar se compila y se instala ejecutando en la terminal los siguientes comandos.

#cd snort-2.9.9.0 --with-mysql
#./configure
#make
#make install

Dicho proceso se puede apreciar en la siguiente figura.

Figura 9. Instalación de Snort



Fuente. El Autor

7.5.2 Configuración de Snort. Como primer paso se deben crear las carpetas donde va a funcionar snort. Para esto se utilizaran comandos en la terminal de Linux. Por lo tanto se mostraran los comandos utilizados en cada paso.

#mkdir /etc/snort

Ahora dentro de la carpeta creada de snort, se agrega otra carpeta donde se almacenen las firmas que se descargaran de la página de la aplicación.

#mkdir /etc/snort/rules

Luego en la ruta donde se guardan los log de Centos, se crea una carpeta de snort para almacenar los registros de actividad del sistema de snort.

#mkdir /var/log/snort

También se requiere crear un usuario snort, y darle los permisos de ese usuario a dicha carpeta creada anteriormente.

#adduser snort

#chown snort /var/log/snort

El fichero de configuración local se crea en la carpeta sysconfig de la carpeta etc.

#touch /etc/sysconfig/snort

Ahora el ejecutable se copia a su directorio de trabajo

#cp /usr/local/bin/snort /usr/sbin

La siguiente figura muestra la ejecución de dichos comandos.

Figura 10. Creación de carpetas de snort

```
[root@CentosSpark snort-2.9.9.0]# cd
[root@CentosSpark ~]# mkdir /etc/snort
[root@CentosSpark ~]# mkdir /etc/snort/rules
[root@CentosSpark ~]# mkdir /var/log/snort
[root@CentosSpark ~]# adduser snort
[root@CentosSpark ~]# chown snort /var/log/snort
[root@CentosSpark ~]# touch /etc/sysconfig/snort
[root@CentosSpark ~]# cp /usr/local/bin/snort /usr/sbin
```

Fuente. El Autor

Además también, se hace necesario copiar ciertos archivos extraídos de la carpeta snort, a la ruta de la carpeta del sistema snort. Dichos archivos son snort.conf, unicode.map, classification.config, sid-msg.map, gen-msg.map. A continuación los comandos utilizados.

#cp /root/snort-2.9.9.0/etc/snort.conf /etc/snort/
#cp /root/snort-2.9.9.0/etc/unicode.map /etc/snort/
#cp /root/snort-2.9.9.0/etc/classification.config /etc/snort/
#cp /root/snort-2.9.9.0/etc/sid-msg.map /etc/snort/
#cp /root/snort-2.9.9.0/etc/gen-msg.map /etc/snort/

Seguido se realizó registro en la web de snort, para poder descargar las firmas oficiales y se descomprimen en la carpeta /etc/snort/rules creada anteriormente.

#cp rules/ /etc/snort/rules/*

Además se crea la carpeta donde se van a guardar los preprocesadores de snort, ejecutando el comando.

#mkdir etc/snort/preproc_rules

Los preprocesadores de la carpeta extraída se copiaron a la ruta de la carpeta creada anteriormente, dentro de la carpeta snort.

#cp /root/snort-2.9.9.0/preproc_rules/ /etc/snort/preproc_rules/*

Los objetos precompilados para la versión 6.9 de CentOS se copian en la respectiva carpeta.

#cp so_rules/precompiled/RHEL-6-0/i386/2.9.4.0/ /usr/local/lib/snort_dynamicrules/*

El fichero de configuración de snort, ubicado en la ruta /etc/snort/snort.conf permite configurar el sistema para asignar el rango de direcciones de red, ruta de las librerías, y configurar las reglas, dentro de otras funciones. Como se evidencia en las siguientes figuras.

Se especifica el rango de direcciones ip de la red interna de la Alcaldía, modificando la variable HOME_NET: var HOME_NET o ANY. Para editar dicho archivo se abre a través del editor Gedit, por lo que se ejecuta el comando en consola que se aprecia seguidamente.

#gedit /etc/snort/snort.conf

Modificando la variable HOME_NET por el rango de direcciones de la red.

Figura 11. Configurando la red en snort

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.88.1/24
```

Fuente: El Autor

Seguido se edita el directorio donde se encuentran almacenadas las reglas, modificando la variable: var RULE_PATH /etc/snort/rules, directorio que se creó en pasos anteriores.

Figura 12. Configuración de reglas

```
var RULE_PATH /etc/snort/rules
```

Fuente. El autor

El directorio donde se encuentran los preprocesadores se especifica:
var PREPROC_RULE_PATH /etc/snort/preproc_rules

Figura 13. Configurando preprocesadores

```
var PREPROC_RULE_PATH /etc/snort/preproc_rules
```

Fuente. El autor

Luego de editar el archivo snort.conf se guardan los cambios y se prueba con el comando *#snort -T -c /etc/snort/snort.conf*
Al realizar la prueba visualiza la siguiente figura, donde se evidencia su correcto funcionamiento.

Figura 14. Probando Snort

```
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>

Snort successfully validated the configuration!
Snort exiting
[root@CentosSpark ~]# snort -T -c /etc/snort/snort.conf
```

Fuente. El Autor

7.5.3 Instalación de MySql. El gestor de base de datos Mysql se utilizara para almacenar los datos de las alertas generados por snort, y que también será utilizada por aplicaciones web que visualizaran los datos de dichas alertas.
Para instalar el servidor MySql se deben de ejecutar los siguientes comandos:

#yum install mysql-server
#yum install mysql-devel

Para iniciar el servidor MySQL se ejecuta

#service mysqld start

Se conecta al servidor MySQL a través de la terminal.

#mysql –u root –p

Se realiza una prueba a continuación para verificar que el motor de base de datos se encuentra instalado, y así mismo se crean el usuario de snort, la base de datos y permisos necesarios para su funcionamiento.

Figura 15. Conectando a servidor Mysql

```
[root@CentosSpark ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.1.73 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
```

Fuente. El autor

Seguido se le brindan todos los privilegios al usuario root, indicándole una contraseña de acceso:

*#GRANT ALL PRIVILEGES ON mysql.*TO root@localhost IDENTIFIED BY 'test';*

Se crea la base de datos de snort:

create database snort;

A continuación se crean las tablas para la base de datos de snort, importándolas del archivo create_mysql, extraída del subdirectorio /schemas de la aplicación barnyard, que se instaló anteriormente.

Se ejecuta para ello el comando:

#mysql -u root -p snort </root/create_mysql

Se ingresa al servidor Mysql, e introduce la contraseña, en este caso test, para comprobar que se han creado las tablas correctamente, para esto se realizaron los siguientes pasos.

#mysql -u root –p snort

Se introduce la contraseña a continuación.
Se selecciona la base de datos snort

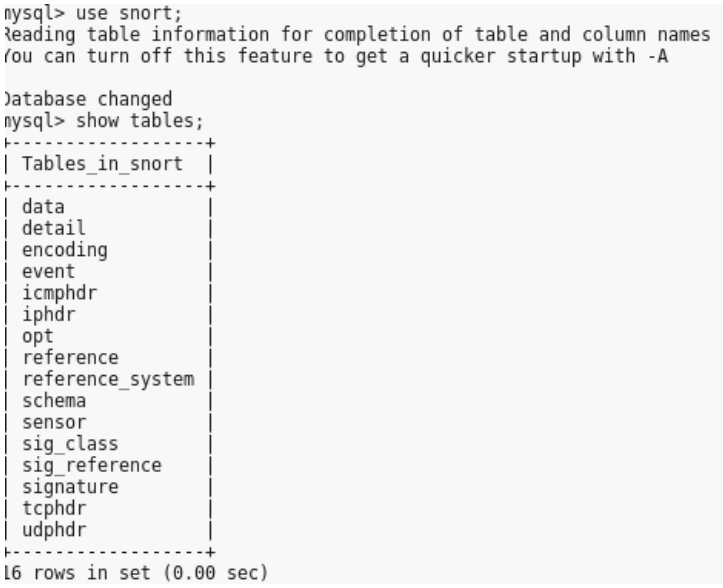
> use snort;

Para ver las tablas que se han creado para nuestra base de datos snort se ejecuta:

> show tables;

La ejecución de dichos comandos se podrá apreciar en la figura de la siguiente figura.

Figura 16. Tablas base de datos snort



Fuente. El autor

7.5.4 Instalación de Barnyard. Esta es una aplicación que toma los archivos de registro de Snort y los procesa para luego guardar los datos en la base de datos de snort que se creó anteriormente en mysql.
Para su instalación se descarga el paquete comprimido de la página https://github.com/firnsy/barnyard2/archive/v2-1.13.tar.gz.
Una vez descargado se procede a descomprimir con el comando en consola.

#tar –xzvf v2-1.13.tar.gz

Seguido se ingresa a la carpeta extraída con el comando

#cd barnyard2-2-1.13

Dentro de la carpeta se compila, se configura con la librería de mysql, y se instala con los siguientes pasos.

 # ./autogen.sh
 # ./configure -with-mysql -libraries=/usr/lib/mysql/
 # make
 # make install

A continuación se requiere que el archivo de configuración de barnyard se copie en la ruta de snort.

 # cp etc/barnyard2.conf /etc/snort

También se crea una carpeta dentro de la carpeta de registro (log), donde se almacenara un archivo Waldo (archivo en blanco).

#mkdir /var/log/barnyard2

A dicha carpeta se le dan permisos para que sea modificable.

#chmod 666 /var/log/barnyard2

Se crea el archivo en blanco requerido para barnyard2 en la carpeta de snort dentro del directorio log.

 # touch /var/log/snort/barnyard2.waldo

Es necesario también copiar el archivo de configuración de barnyard2, a la ruta de instalación de snort.

 # cp etc/barnyard2.conf /etc/snort

Para finalizar es necesario configurar el archivo de configuración de barnyard2, copiado en la ruta de snort. Primero se ubica en la ruta del archivo, y seguido se abre el archivo con el editor gedit. Para ello se ejecuta en consola las siguientes líneas.

#cd /etc/snort/
#gedit barnyard2.conf

Dicho archivo de configuración barnyard2.conf consta de tres bloques de configuración, en donde la primera parte se declaran las variables, seguido la configuración de entrada, y por último la configuración de salida de los datos.
Inicialmente se ubican los archivos de configuración de snort, verificando que se encuentren en el directorio de snort. Seguido se presenta la figura donde se visualiza dichos pasos.

Figura 17. Configurando el archivo de barnyard

```
config reference_file:      /etc/snort/reference.config
config classification_file: /etc/snort/classification.config
config gen_file:            /etc/snort/gen-msg.map
config sid_file:            /etc/snort/sid-msg.map
```

Fuente. El autor

Luego se descomenta la siguiente línea para ubicar el directorio de salida de barnyard.

config logdir: /var/log/barnyard2

En las líneas donde se declaran las variables del equipo y de la interfaz de red, se descomentan y editan, dando los datos correspondientes, como se muestran seguidamente.

config hostname: localhost
config interface: eth0

Se declara la ruta donde se encuentra el archive waldo, en la carpeta log.

config waldo_file: /var/log/snort/barnyard2.waldo

En el segundo bloque de configuración del archivo de barnyard, no se realizan cambios, dado que solo existe un tipo de entrada para dicho archivo, así que se establece por defecto.

Para terminar, en el último bloque del archivo se declara las variables de la base de datos de snort, se crea una nueva línea, dando los parámetros de la base de datos, como se aprecia en la siguiente figura.

Figura 18. Parámetros de la base de datos en barnyard

```
output database: log, mysql, user=root password=test dbname=snort host=localhost
```

Fuente. El autor

Finalizando la configuración de barnyard, se guardan los cambios realizados en el archivo de configuración barnyard2.conf.

7.5.5 Instalación de Apache. Para la instalación de apache se ejecuta desde línea de comando la siguiente línea.

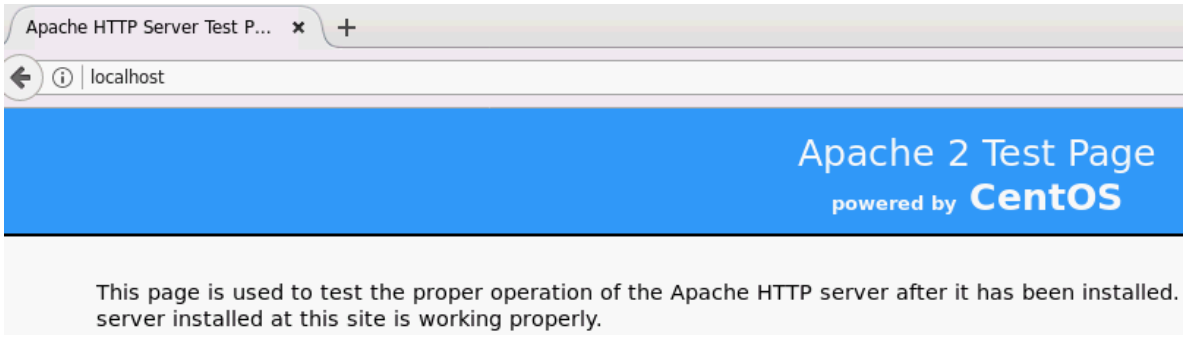
#yum install httpd

A continuación se inicia el servidor en la terminal con el comando que se muestra a continuación.

#service httpd start

Seguidamente se escribe la dirección http://localhost en el navegador y se podrá visualizar que el servidor apache funciona correctamente, como se muestra en la figura 19.

Figura 19. Instalación de apache



Fuente. El Autor

Así también se necesita de la librería php-mysql para realizar conexiones la base de datos mysql Al igual que se necesita el lenguaje php, para dar soporte al servidor web apache instalado anteriormente.

#yum install php-mysql
#yum install php

7.5.6 Instalación de Base. Se realizó la instalación de php y apache, que son requeridos para que pueda funcionar base, el cual no es más que una interfaz gráfica que permite visualizar y analizar las intrusiones detectadas y almacenadas por snort, este los procesa para mostrarlos cómodamente a través de su interfaz. Seguidamente se presentan los pasos que se siguieron para su instalación.

En primer lugar se descarga el paquete base-1.4.5.tar.gz desde la página web: http://base.secureideas.net/.

A continuación se descomprime el paquete en el directorio /var/www/html:

#cp base-1.4.5.tar.gz /var/www/html
#cd /var/www/html
#tar xvfz base-1.4.5.tar.gz
#mv base-1.4.5 base

Se ha copiado la carpeta de base a la carpeta www del servidor apache. Pero con esto no es suficiente para que funcione, además se requirió tener instalado los paquetes *Adodb* e *Image_Graph.*

Para instalar *Adodb* hay que realizar los siguientes pasos:

Se descarga el paquete adodb5.20.9 de la página http://adodb.sourceforge.net

Se descomprime el paquete y se copia dentro de la carpeta /var/www/:

#tar xvfz adodb-5.20.9.tar.gz
#mv ./adodb /var/www/ html/
#mv ./adodb /var/www/

También es necesario realizar instalación de los siguientes elementos, para que Base pueda graficar.

#yum install php-pear
#pear install Image_Canvas-alpha
#pear install Image_Color
#pear install Numbers_Roman
#pear install Image_Graph-0.8.0

Se inicia el servidor web a través del comando en consola, en el cual el servicio de apache es *httpd*.

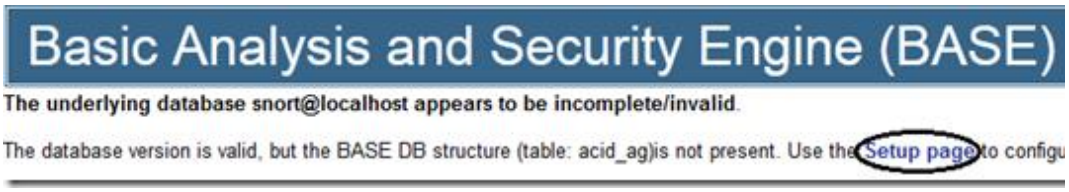
#service httpd start

Se accede a la página Web de BASE, a través de un navegador web, indicando la ip local del servidor o localhost, seguido de la carpeta de Base.

http://localhost/base

Muestra la siguiente pantalla al iniciar, donde se procede a configurar a través de la opción Setup Page.

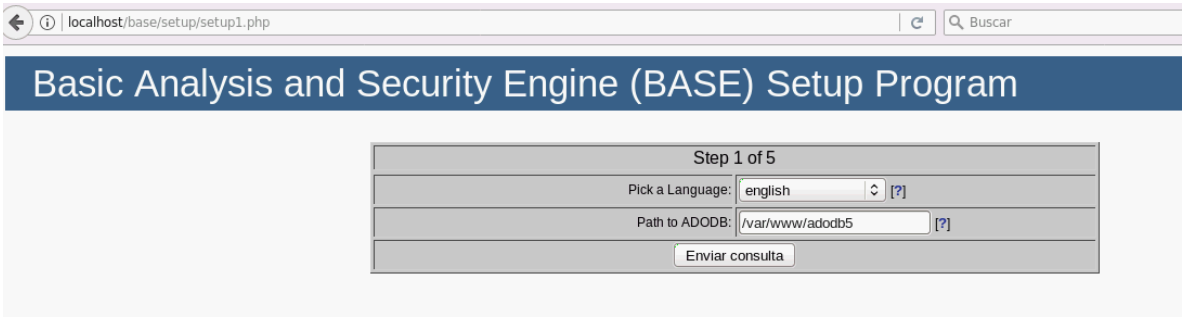
Figura 20: Pantalla de Base



Fuente. El Autor

Seguido se configuro la ruta a adodb alojada en la carpeta de apache www, como se muestra seguidamente.

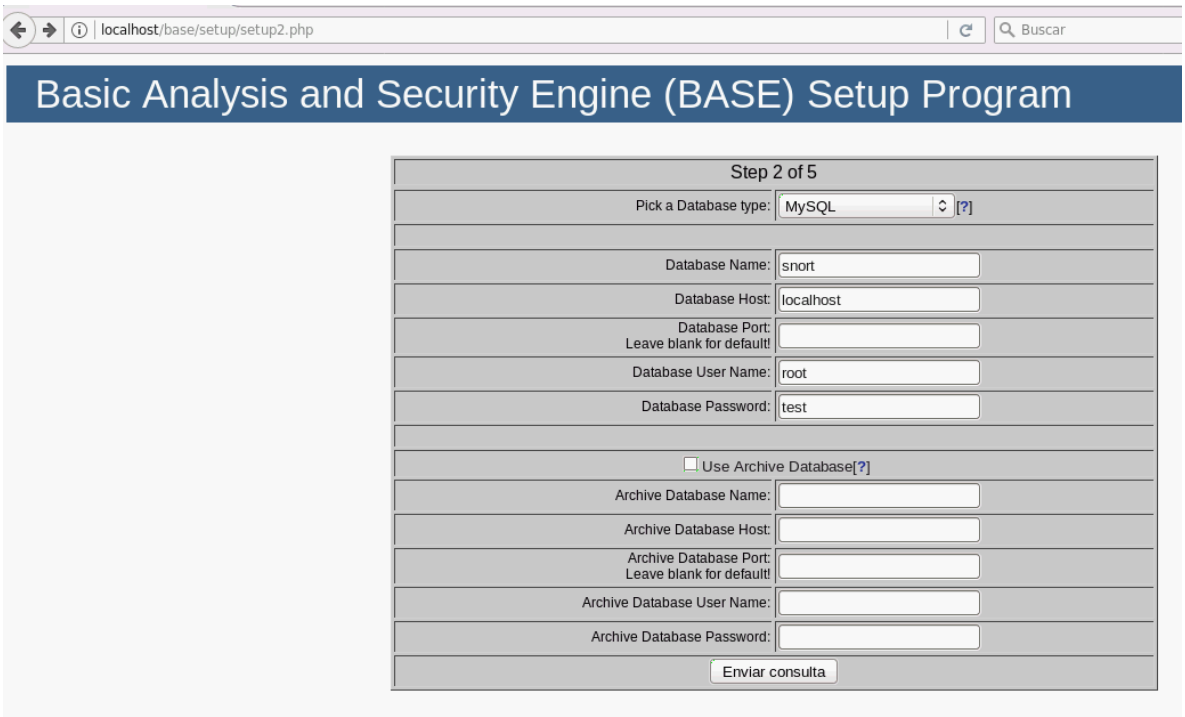
Figura 21: Configurando Base



Fuente. El Autor

En el siguiente paso de la configuración, se configuran los datos de la base de datos, como el nombre de la base de datos, host, usuario, contraseña, y a continuación se envía la consulta.

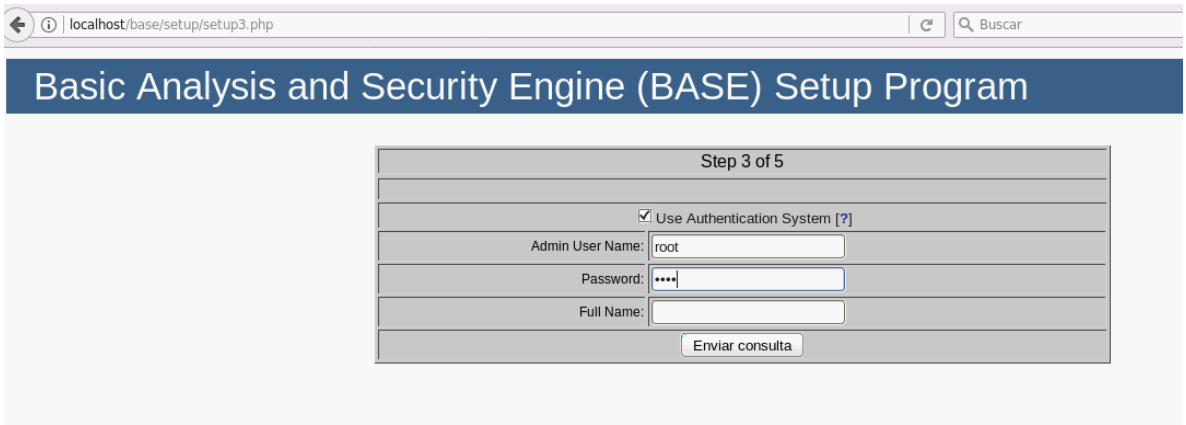
Figura 22. Configurando la base de datos en base



Fuente. El Autor

A continuación se presenta la siguiente pantalla donde se solicita los datos de usuario para iniciar sesión y conectarse a la base de datos creada en Mysql.

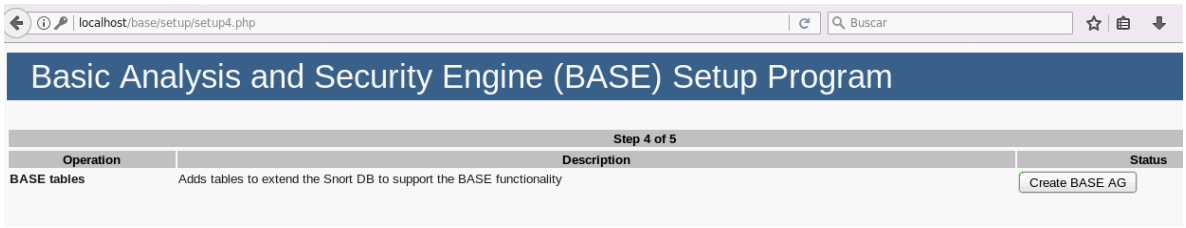
Figura 23. Finalizando la configuración de Base



Fuente. El Autor

Seguido se muestra la siguiente figura donde se presiona Create Base AG, para que agregue tablas a la base de datos Snort.

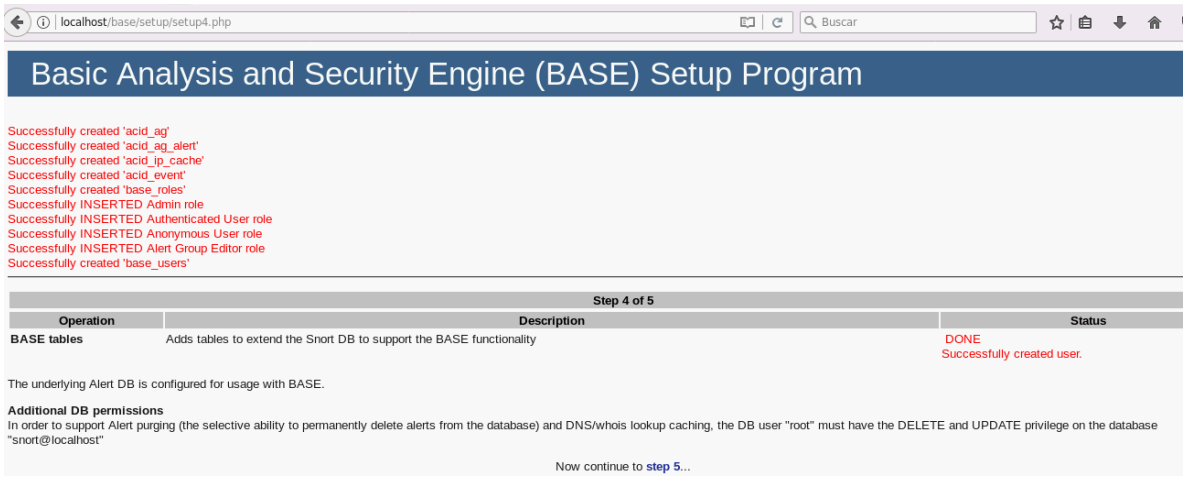
Figura 24. Agregando tablas a Snort



Fuente. El Autor

Al finalizar el proceso que se inició en el paso anterior, se visualiza la siguiente figura, donde se aprecia que el proceso finalizo y que fue exitoso.

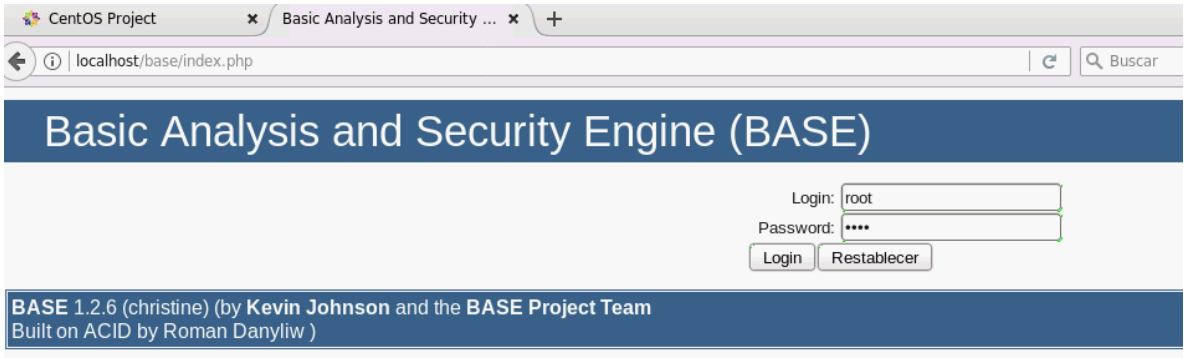
Figura 25. Proceso finalizado de Base



Fuente. El Autor

Una vez finalizado el proceso, solicita iniciar sesión con los datos previamente establecidos como son el usuario y contraseña, así como se presenta en la siguiente figura.

Figura 26. Iniciando sesión en Base



Fuente. El Autor

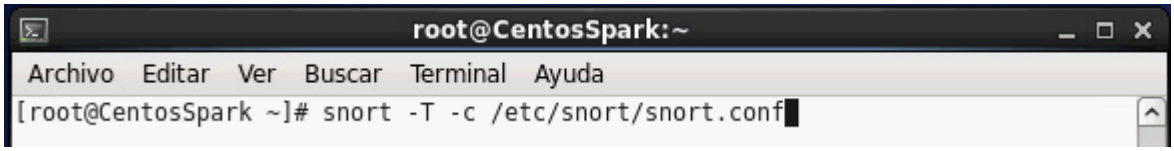
Una vez iniciada sesión en Base, se puede acceder a la información almacenada de snort en la base de datos, al igual que permite visualizar las alertas que se generan.

8. PRUEBAS DEL IDS EN LA RED DE DATOS DE LA ALCALDÍA DE MONTERÍA.

Se realizaron las instalaciones y configuraciones de las herramientas y aplicaciones necesarias para el correcto funcionamiento del sistema de detección de intrusos con Snort, al igual que la configuración de la red. Para que el sistema funcione, se necesita iniciar los servicios de las aplicaciones, como es el caso de mysql, apache y por ultimo snort.

Pero antes de iniciar los servicios de las aplicaciones, específicamente Snort permite realizar un test o prueba de que se encuentra instalado correctamente, especificándole además la ruta del archivo .conf que se configuro anteriormente. La figura a continuación muestra el comando utilizado para dicha prueba.

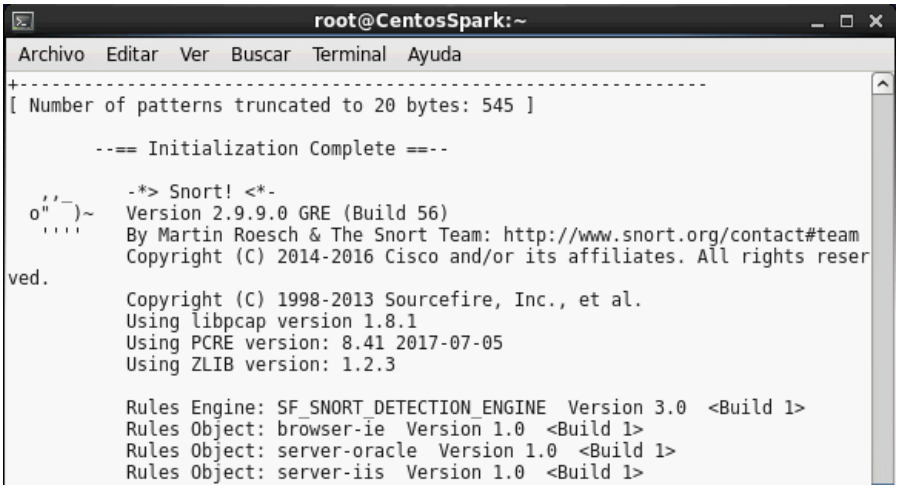
Figura 27. Probando Snort



Fuente. El Autor

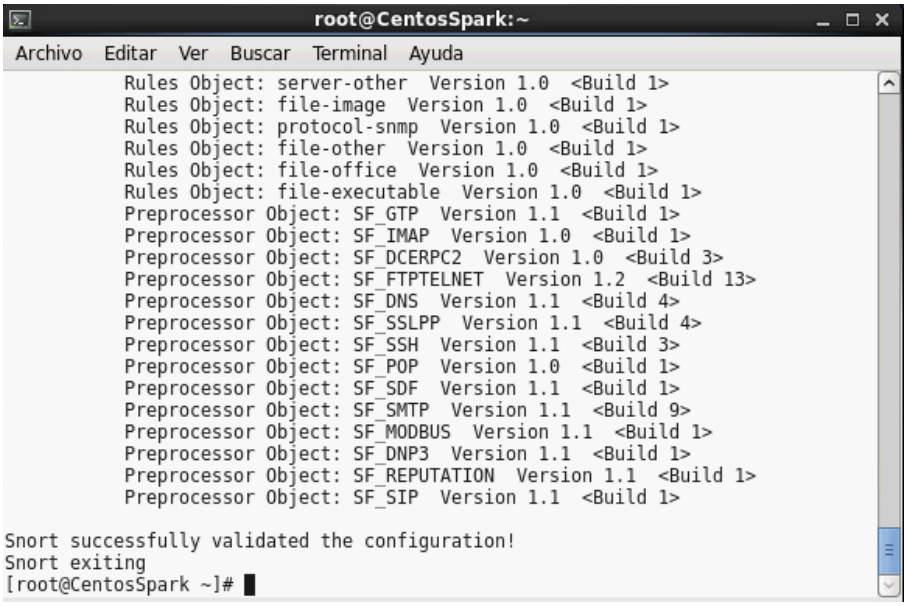
Una vez ejecutado el comando en consola, inicia el proceso de prueba verificando cada uno de los elementos detallados en el archivo de configuración, como se aprecia en las siguientes figuras.

Figura 28. Proceso de pruebas de Snort



Fuente. El Autor

Figura 29. Pruebas de Snort satisfactoria



Fuente. El Autor

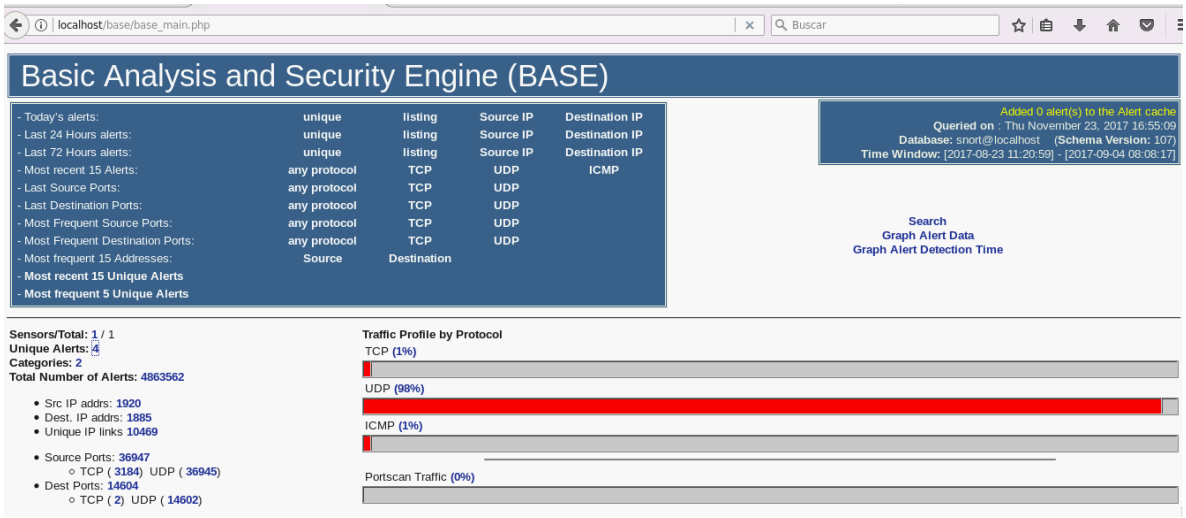
Finalizada la prueba de verificación de snort, se muestra que se validó la configuración satisfactoriamente.

Continuando con los servicios, se requirió de los siguientes comandos en consola, en el orden que se han mencionado.

#service mysqld start
#service httpd start
#service snortd start

Iniciado dichos servicios, se ha mantenido en funcionamiento por varios días, para la recolección de datos, y luego analizar los datos obtenidos.

Figura 30. Análisis de Base



Fuente. El Autor

En un primer inicio de la aplicación Base se puede verificar el análisis de la información que toma base de la base de datos snort. Permitiendo visualizar en primera instancia el análisis de tráfico por Tcp (1%), Udp (98%), e Icmp (1%).

Del lado izquierdo aparece un panel que detalla en resumen por elementos, el número de sensores funcionando, alertas detectadas, total de alertas, así como también las direcciones de ip que intervienen, sean de fuente o de destino.

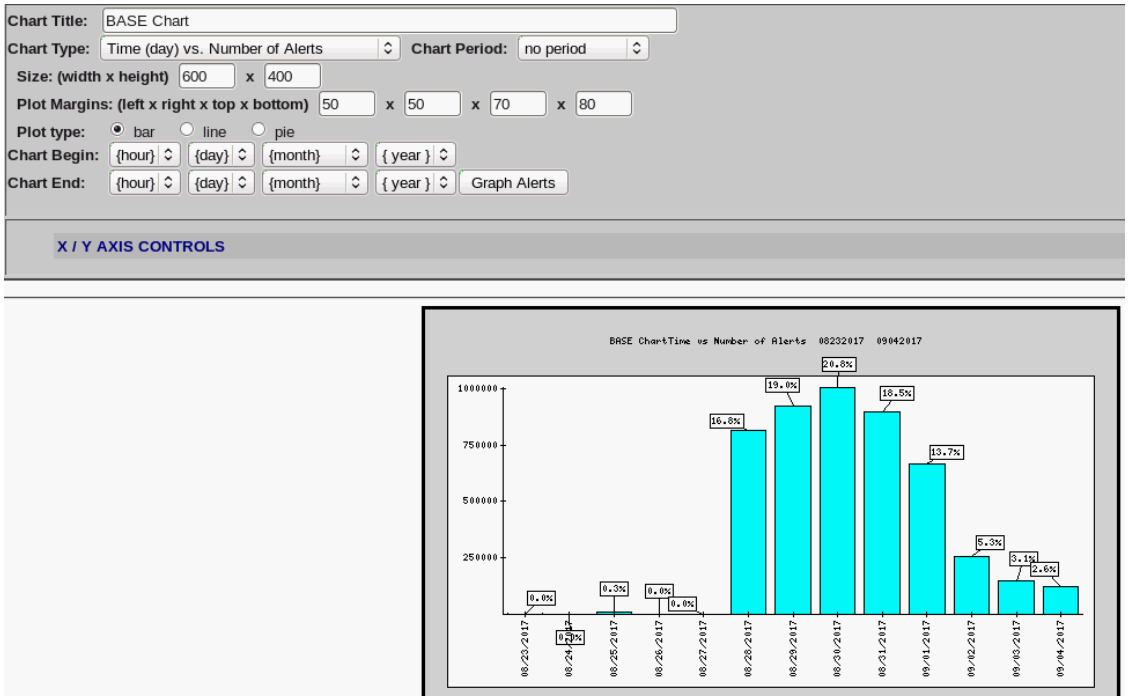
Otro dato importante que detalla es el número de alertas únicas, cuatro en este análisis, agrupándolas en 2 categorías. Así mismo el número total de alertas (4863562), número total de escaneo de puertos, entre otros datos. Seleccionando cada una de las opciones que muestra el menú, se puede visualizar información

detallada de cada una de estas, permitiendo realizar un análisis más exhaustivo de los datos capturados.

Para que se establezca una alerta a través de los paquetes capturados, es necesario que el motor de detección actué por medio de la información que captura el decodificador de paquetes libcap. El motor de detección se encarga de detectar si alguna actividad de intrusión existe en un paquete, utilizando las reglas que han sido definidas para este propósito. Las reglas son verificadas contra todos los paquetes. Si un paquete cumple con la definición de la regla, el sistema de alertas generara un log o una alerta almacenada en la base de datos de mysql.

La visualización de los datos obtenidos, se da por parte de la opción Graph Alert Data, el cual permite graficar los datos según las opciones que el usuario necesite. Un ejemplo de estos es la gráfica que se obtiene del número de alertas que se generaron en un día. Dicho ejemplo se puede apreciar en la siguiente figura.

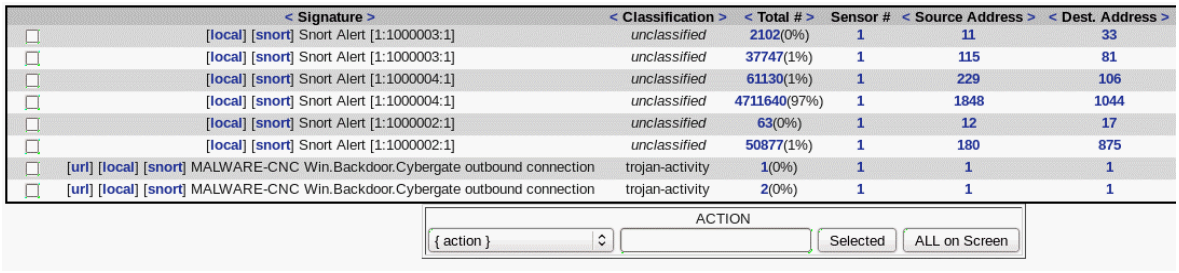
Figura 31. Número de alertas que se presentan por día



Fuente. El Autor

Dentro de las alertas que se generaron al ejecutar el sistema de detección de intrusos se pudo evidenciar las siguientes alertas, como se muestra en la siguiente figura.

Figura 32. Alertas generadas



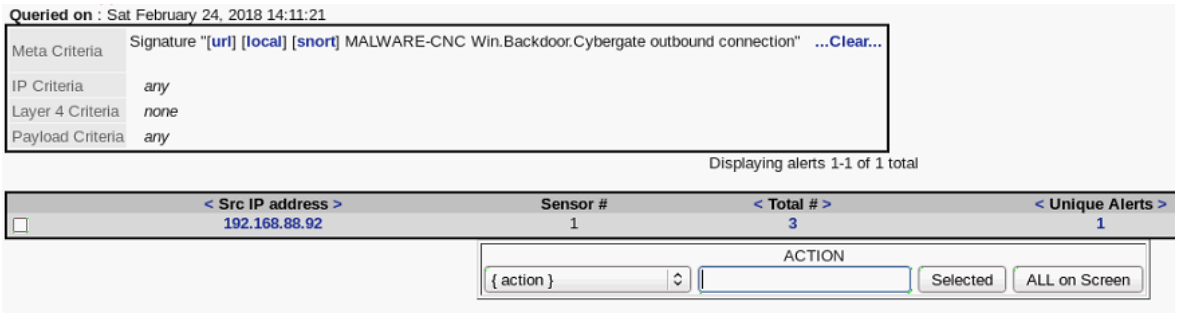
< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >
[local] [snort] Snort Alert [1:1000003:1]	unclassified	2102(0%)	1	11	33
[local] [snort] Snort Alert [1:1000003:1]	unclassified	37747(1%)	1	115	81
[local] [snort] Snort Alert [1:1000004:1]	unclassified	61130(1%)	1	229	106
[local] [snort] Snort Alert [1:1000004:1]	unclassified	4711640(97%)	1	1848	1044
[local] [snort] Snort Alert [1:1000002:1]	unclassified	63(0%)	1	12	17
[local] [snort] Snort Alert [1:1000002:1]	unclassified	50877(1%)	1	180	875
[url] [local] [snort] MALWARE-CNC Win.Backdoor.Cybergate outbound connection	trojan-activity	1(0%)	1	1	1
[url] [local] [snort] MALWARE-CNC Win.Backdoor.Cybergate outbound connection	trojan-activity	2(0%)	1	1	1

ACTION { action } Selected ALL on Screen

Fuente: El autor

Se puede evidenciar que una de las alertas generadas corresponde a la clasificación de “Trojan activity” es decir actividad de un troyano del tipo de Backdoor o que se infectó por puerta trasera; en la siguiente figura se observa a detalle la ip desde donde se genera la alerta, el sensor que la detecto, y las veces que ocurrió.

Figura 33. Detalle de alerta generada



Queried on : Sat February 24, 2018 14:11:21

Meta Criteria	Signature "[url] [local] [snort] MALWARE-CNC Win.Backdoor.Cybergate outbound connection" ...Clear...
IP Criteria	any
Layer 4 Criteria	none
Payload Criteria	any

Displaying alerts 1-1 of 1 total

< Src IP address >	Sensor #	< Total # >	< Unique Alerts >
192.168.88.92	1	3	1

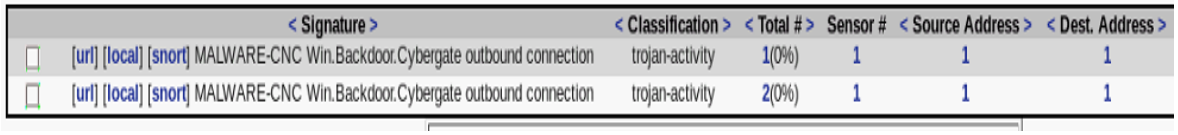
ACTION { action } Selected ALL on Screen

Fuente: El autor

Otra de las alertas generadas, también corresponde al mismo tipo de trojan, en donde se evidencia la actividad de un malware que afecta una máquina de la red de la alcaldía y que puede afectar a varios equipos y poner en riesgo la información de los usuarios.

Seguido se observa el detalle de la alerta generada en la figura 34.

Figura 34. Detalle de alerta



< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >
[url] [local] [snort] MALWARE-CNC Win.Backdoor.Cybergate outbound connection	trojan-activity	1(0%)	1	1	1
[url] [local] [snort] MALWARE-CNC Win.Backdoor.Cybergate outbound connection	trojan-activity	2(0%)	1	1	1

Fuente: el autor

Para este tipo de alertas generadas por el sistema, se deben realizar un plan de acción inmediato que permita eliminar dichas amenazas de la red. Verificando en cada uno de los equipos infectados la eliminación total de dicho Malware.
Luego de eliminado el malware se desactivan dichas alertas del sistema, y se escanea nuevamente la red en busca de nuevas intrusiones o anomalías en la red.

Con este análisis de la red se evidencio que las soluciones instaladas como firewall o cortafuego físico y antivirus, no son suficientes para evitar los ataques informáticos con malware, que ponen en alto riesgo la seguridad de la información. Con la implementación del sistema de detección de intrusos se brinda una capa adicional de seguridad a las redes, permitiendo a los administradores de sistemas una rápida actuación bajo las alertas generadas por el sistema.

9. RESULTADO A ENTREGAR

Se realizará la entrega de un sistema de detección de intrusos puesto en marcha en la red interna de la alcaldía de Montería, para lo cual se utilizará el software libre Snort, que se ejecuta en plataformas Linux, por lo que se es necesario contar con un equipo servidor.

Gracias a que Snort que es un sistema de detección de intrusos basados en red, el cual proporciona alertas y notificaciones ante accesos no autorizados a la infraestructura informática interna, se lograría alcanzar los objetivos planteadas en el presente proyecto.

10. RECURSOS PARA EL DESARROLLO

Los recursos necesarios para el desarrollo del presente proyecto son suministrados por los investigadores, entre los que se destacan los siguientes:

- Computador portátil e impresora para la trascripción de la propuesta y los resultados del trabajo de investigación, implementación de las prácticas para poner en marcha la propuesta y ejecución de la versión final del proyecto.

Tabla 1. Precios equipos Portátiles

Equipo	Cantidad	Valor
Portatil Hp Pavilion G	1	1,350.000 $
Hacer V3-471	1	1,300.000 $
Impresora Hp	1	200.000 $
	Total	2,850.000 $

Fuente. El Autor

- Servidor o computador de buenas especificaciones en donde implementar varias aplicaciones, este equipo es de segunda que funciona correctamente. Además de un equipo de pruebas y consultas.

Tabla 2: Precio equipos servidor y pruebas

Equipo	Cantidad	Valor
Hp Proliant ML350 G4	1	1,250.000 $
Hp ProOne 400	1	1,700.000 $
	Total	2,950.000 $

Fuente: El Autor

- Investigadores de desarrollo del proyecto. El esfuerzo de tiempo y costos del proyecto para su desarrollo correctamente, gastos de alojamiento, manutención entre otros, están incluidos en la tabla de personal reflejados en el valor de horas y estos estarán a cargo por cuenta del investigador.

Tabla 3. Precio horas de investigador del proyecto.

Investigador	Estudio	Horas	Valor	Tiempo	Total
Jayner Quintero Herrera	Ingeniero en Informática	6	35.000$	16 Semanas	7,200.000$
				Total	7,200.000$

Fuente. El Autor

- Información digital en el internet, libros especializados.
  Se refiere a bibliografía en donde el investigador consulta la información sea en fuentes de internet o libros, para el análisis del proyecto, la cual estará a cargo de los mismos ya que son instrumento fundamental para el análisis y creación del proyecto.

Tabla 4. Recursos bibliográficos

Concepto	Descripción	Total
Acceso Internet	110.000$ x mes	440.000 $
Libros	2 x 100.000	200.000 $
	Total	640.000 $

Fuente. El Autor

11. CONCLUSIONES

Con la revisión de la red actual de la alcaldía de montería, se pudo evidenciar la necesidad de agregar otro nivel de seguridad, a través de una herramienta que permitiera detectar intrusiones que hayan sobrepasado la primera barrera de seguridad, en este caso el firewall.

Luego de un análisis de los tipos de ids, dentro de los que se encontraron de tipo host y de red, así como también pagos y otros open source; se pudo determinar inicialmente el tipo de ids a implementar; que para la Alcaldía de Montería requería del tipo red que realizara análisis y monitoreo de toda la organización. Además que se encontraron gran variedad de herramientas de tipo de código abierto, que cumplían con las exigencias y requisitos de la implementación, adaptándose y configurándose al desarrollo del proyecto.

Con la implementación del sistema de detección de intrusos a través de herramientas de software libre, se cuenta con un servidor que monitorea el tráfico de la red de la Alcaldía de Montería. Este tráfico queda almacenado en la base de datos de mysql, con lo que se dispone de un registro histórico de todo lo que ha sucedido desde su implementación, con lo que se dispone de una herramienta de auditorías, identificando las direcciones ip de origen, destino, así como los puertos y protocolos escaneados en el tráfico.

El sistema de detección de intrusos requiere monitorización continua por parte de los administradores de la red, para dar aviso a los usuarios de las maquinas, dado que el sistema por sí solo no es capaz de dar aviso o identificar si tuvo éxito o no la intrusión.

Toma gran importancia el haber desarrollado el proyecto a través de herramientas de software libre, desde el sistema operativo pasando por bases de datos, hasta otras herramientas complementarias que integran el sistema de detección, brindando múltiples posibilidades de adaptación y configuración, disminuyendo en gran medida los costos de implementación de dicho sistema.

12. RECOMENDACIONES

Existen muchas aplicaciones que ofrecen soluciones a los servicios que se desean implementar, pero hay que tener en cuenta que todas no se adaptan o no son adecuadas a nuestra infraestructura de red. Por lo que se requiere analizar con detalle lo que se requiere hacer. En este caso se recomienda realizar una adaptacion adicional de un sistema de prevencion de intrusos al sistema ya desarrollado.

Implementar adicionalmente un sistema de deteccion de intrusos del tipo host que sea ubicado delante del firewall, permitiendo ser un filtro de todos los ataques posibles, al igual que disminuye la actividad sospechosa que entraria a la red. Dando paso a que el segundo ids permita identificar los ataques que no fueron detectados.

Continuar con la implementación de IDS en las demás redes externas de la institución y expandir el sistema de detección creando más sensores y una base de datos centralizada. Orientado a los Sistemas de Detección de Intrusos Distribuidos.

Analizar los patrones de los ataques desconocidos con la finalidad de crear nuevas reglas que nos permitan actualizar nuestra base de datos de reglas.

13. DIVULGACIÓN

Dicho proyecto ha sido inicialmente socializado y divulgado a traves del personal de la oficina de sistemas de la Alcaldia de Monteria; desde el personal tecnico hasta el coordinador de la oficina, resaltando las bondades que trae consigo la implementacion del sistema deteccion de intrusos.

Adicionalmente se realizara publicacion de dicho proyecto en el repositorio institucional de la Unad.

14. BIBLIOGRAFIA

Ataques Informáticos. [En Línea]. [Revisado 9 Abril de 2017]. Disponible en Internet: https://sites.google.com/site/sykrayolab/ataques-informaticos

BORGHELLO, Cristian. Amenazas Lógicas - Tipos de Ataques. [En Línea], 2009. [Revisado 6 Septiembre de 2017]. Disponible en Internet: http://www.segu-info.com.ar/ataques/ataques.htm

BORGHELLO, Cristian. Detección de Intrusos en Tiempo Real. [En Línea]. 2009. [Revisado 6 de Septiembre de 2017]. Disponible en Internet: http://www.segu-info.com.ar/proteccion/deteccion.htm

BONILLA, Sandra. GONZALEZ, Jaime. Modelo de la seguridad de la información. En: Ingenierías USBMed. Enero – Junio, 2012, vol. 3, no. 1, p. 7Tomado de http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1.pdf

COLOMBIA, CONGRESO DE LA REPUBLICA, Ley 1273, (05, 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". Diario Oficial, Bogotá, D.C., 2009, No. 47.223, p. 5-6.

Ecured, Ataque Informático. [En Línea]. 2012. [Revisado 9 Abril de 2017}. Disponible en Internet: https://www.ecured.cu/Ataque_inform%C3%A1tico

GUTIERREZ, Leonardo. Curso de Ciberseguridad y Hacking Ético 2013, España: Punto Rojos Libros. 2014. 574p

JORGE ADAIR LARIOS ESCAMILLA, RODRIGO JULIAN SANCHEZ GONZALEZ. Ciberdelito, Ingeniero en Telecomunicaciones. Trabajo de Grado. México, D.F.: Universidad Nacional Autónoma de México. Facultad de Ingeniería. 2014. 154p.

MIERES, Jorge, Ataques informáticos. [En Línea]. Enero 2009. [Revisado 6 de Septiembre de 2017]. Disponible en Internet: https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

Red Hat, Manual de seguridad. [En Línea]. 2005. [Revisado 6 Septiembre de 2017] Disponible en Internet: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html

15. ANEXOS

RESUMEN ANALÍTICO ESPECIALIZADO - RAE	
Información	
Tema	El tema se engloba dentro del campo de proyectos tecnológicos aplicados, en el aspecto de la seguridad informática.
Titulo	Implementación de un sistema de detección de intrusos en la red interna de la alcaldía de montería usando software libre.
Autor	Jayner Ahmed Quintero Herrera
Fuentes bibliográficas	Se realiza la consulta a diferentes fuentes, aquí solo algunas principales. - BORGHELLO, Cristian. Detección de Intrusos en Tiempo Real. [En Línea]. 2009. [Revisado 6 de Septiembre de 2017]. Disponible en Internet: http://www.segu-info.com.ar/proteccion/deteccion.htm - BONILLA, Sandra. GONZALEZ, Jaime. Modelo de la seguridad de la información. En: Ingenierías USBMed. Enero – Junio, 2012, vol. 3, no. 1, p. 7 Tomado de http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1.pdf - COLOMBIA, CONGRESO DE LA REPUBLICA, Ley 1273, (05, 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". Diario Oficial, Bogotá, D.C., 2009, No. 47.223, p. 5-6. - JORGE ADAIR LARIOS ESCAMILLA, RODRIGO JULIAN SANCHEZ GONZALEZ. Ciberdelito, Ingeniero en Telecomunicaciones. Trabajo de Grado. México, D.F.: Universidad Nacional Autónoma de México. Facultad de Ingeniería. 2014. 154p.
Año	2018
Resumen	Los diferentes sistemas de información que utiliza la sede principal de la Alcaldía de Montería deben estar disponible todo el tiempo, dado que los sistemas son usados por los usuarios de la entidad, y se llegara a presentar una falla o intrusión, debe ser corregida de inmediato para dar continuidad a los servicios que presta la entidad. Con la implementación de este proyecto se busca beneficiar a los empleados de la entidad, los cuales a través de los activos de información que manejan al interior de la misma, se proveen de mayor seguridad en la disponibilidad, integridad y confidencialidad de los mismos. A la vez que aumenta la confianza en el uso de las herramientas tecnológicas por parte

	de los usuarios, que en muchas ocasiones ven en estas un riesgo de fiabilidad en la información. El desarrollo del proyecto es de gran importancia, dado que el contenido a implementar provee de un gran beneficio para la Alcaldía de Montería, pudiéndose aplicar a las sedes externas de esta entidad que deseen mejorar la seguridad en las redes y sus sistemas informáticos.
Palabras claves	Anomalía, ataques informáticos, Detección de intrusos, ids, snort, seguridad informática, software libre.
Contenidos	Problema Definición del problema, Descripción del problema, Formulación del problema Justificación Objetivos: Objetivo general - Objetivos específicos Marco referencial Antecedentes, Marco contextual, Marco teórico, Marco conceptual Diseño metodológico Metodología de la investigación, Metodología de desarrollo Resultados y discusión Divulgación y recomendaciones Conclusiones

Descripción del problema

Para la Alcaldía de Montería la seguridad es de vital importancia en el correcto funcionamiento de sus redes de datos y de la información que se transmite, por lo que se debe garantizar a través de los pilares de la seguridad, la confidencialidad, integridad y disponibilidad de la información en todo momento. Previniendo que el riesgo de ataques sea reducido o el más mínimo posible, dado que en los últimos años las entidades públicas se han convertido en objetivos de los hackers o personas malintencionadas. Si se llegase a presentar una brecha de seguridad en las redes, podría ocasionar daños irremediables a la integridad de la información, dejando sin servicio a los usuarios finales, o capturando información sensible de la ciudadanía.

El creciente uso y estrategia de las tecnologías de la información plantea a la Alcaldía de Montería la necesidad y compromiso de mejorar las herramientas de seguridad, ya que la información que maneja la entidad debe contener el mínimo de riesgo de pérdida y mayor control en su acceso. Se plantea entonces la oportunidad de implementar un sistema de detección de intrusos para el control de vulnerabilidades para la red interna de la Alcaldía de Montería.

Objetivos

General

Implementar un sistema de detección de intrusos en la red interna de la Alcaldía de Montería, a través de la implementación de diversas herramientas de seguridad informática.

Específicos

- Detallar la situación actual de la red de datos de la Alcaldía de Montería.
- Verificar que IDS es necesario implementar en la red de datos de la Alcaldía de Montería.
- Documentar paso a paso la implementación del IDS en la red de datos de la Alcaldía de Montería.
- Efectuar pruebas que permitan verificar la eficacia del IDS en la red de datos de la Alcaldía de Montería.

Metodología

Para el desarrollo del proyecto se utilizó la metodología PHVA (Planear, Hacer, Verificar y Actuar), la cual plantea la mejora continua.

Planear

Análisis de información de proyectos relacionados, Identificación del estado actual de la red de la alcaldía de Montería, Análisis de las herramientas disponibles para la ejecución del proyecto, Cronograma de actividades

Hacer

Instalación de las librerías necesarias para el correcto funcionamiento del sistema de detección de intrusos. Instalación y configuración del motor de base de datos para el almacenamiento de las alertas del sistema de detección, así como el lenguaje Php, y el servidor de aplicaciones apache. Instalación y configuración del sistema de detección de intrusos con la herramienta Snort, además de la herramienta barnyard.

Verificar

Revisión de cada una de las herramientas y aplicaciones, realizando pruebas que permitieron verificar su correcto funcionamiento. Ajustes requeridos en el documento del proyecto verificando su alineación con los objetivos del proyecto.

Actuar

Para la fase actuar de dicha metodología, se obtuvo como resultado la mejora continua de los dispositivos de red de la oficina de sistemas, a través de la implementación de un sistema de detección de intrusos en la red de la Alcaldía de Montería.

Referentes Teóricos

Los referentes teóricos consultados para el desarrollo del proyecto permitieron la implementación de un sistema de detección de intrusos, dentro de los cuales se encuentra, seguridad, seguridad informática, seguridad en redes, cortafuegos,

sistema de detección de intrusos, arquitectura de un ids, tipos de ids, ids comerciales y de software libre.
Descripción Conceptuales
Se tuvo en cuenta conceptos que ayudaron a conocer las bases de la institución, para una correcta implementación del sistema de detección de intrusiones, entre los cuales se encuentran la organización de la alcaldía, misión, visión; así como también el marco legal relacionado con la detección de intrusos.
Resultados
Se realiza la entrega de un sistema de detección de intrusos puesto en marcha en la red interna de la alcaldía de Montería, para lo cual se utilizará el software libre Snort, que se ejecuta en plataformas Linux, por lo que se es necesario contar con un equipo servidor. Gracias a que Snort que es un sistema de detección de intrusos basados en red, el cual proporciona alertas y notificaciones ante accesos no autorizados a la infraestructura informática interna, se lograría alcanzar los objetivos planteadas en el presente proyecto.
Conclusiones
Luego de un análisis de los tipos de ids, dentro de los que se encontraron de tipo host y de red, así como también pagos y otros open source; se pudo determinar inicialmente el tipo de ids a implementar; que para la Alcaldía de Montería requería del tipo red que realizara análisis y monitoreo de toda la organización. Además que se encontraron gran variedad de herramientas de tipo de código abierto, que cumplían con las exigencias y requisitos de la implementación, adaptándose y configurándose al desarrollo del proyecto. Con la implementación del sistema de detección de intrusos a través de herramientas de software libre, se cuenta con un servidor que monitorea el tráfico de la red de la Alcaldía de Montería. Este tráfico queda almacenado en la base de datos de mysql, con lo que se dispone de un registro histórico de todo lo que ha sucedido desde su implementación, con lo que se dispone de una herramienta de auditorías, identificando las direcciones ip de origen, destino, así como los puertos y protocolos escaneados en el tráfico. El sistema de detección de intrusos requiere monitorización continua por parte de los administradores de la red, para dar aviso a los usuarios de las maquinas, dado que el sistema por sí solo no es capaz de dar aviso o identificar si tuvo éxito o no la intrusión. Toma gran importancia el haber desarrollado el proyecto a través de herramientas de software libre, desde el sistema operativo pasando por bases de datos, hasta otras herramientas complementarias que integran el sistema de detección, brindando múltiples posibilidades de adaptación y configuración, disminuyendo en gran medida los costos de implementación de dicho sistema.

CARTA DE ACEPTACION DE PROYECTO

ALCALDÍA DE
Montería

NIT.800096734

Montería 21 de febrero de 2018

Sres.
Universidad Nacional Abierta y/a Distancia - Unad

Cordial Saludo

Tengo el agrado de dirigirme a ustedes, con la finalidad de hacer de su conocimiento que el Sr. **Jayner Ahmed Quintero Herrera**, Ingeniero de Redes y Soporte de la Alcaldía de Montería, ha desarrollado el proyecto "**IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN LA RED INTERNA DE LA ALCALDIA DE MONTERIA USANDO SOFTWARE LIBRE".** Esto a lo largo del año anterior, a través de diferentes actividades que le permitieron poner en marcha dicho sistema, alojado en servidor de la entidad ubicado en el cuarto de máquinas.

Sin más a que hacer referencia.

Atentamente,

OMAR ACOSTA GOMEZ
Coordinador Oficina de Sistemas
Alcaldía de Montería