Universidad Nacional Autónoma de México

Facultad de Ingeniería

Diseño de Sistema Servidor, e Interfaz para configurar y administrar remotamente el sistema SNORT

TESIS PROFESIONAL
para obtener el título de:

Ingeniería en Computación

PRESENTA:

Jorge Omar Morales Olvera

ASESOR DE TESIS

Ing. Germán Santos Jaimes

México, D.F., Marzo 2004

Agradecimientos

Primeramente, quisiera agradecer, de manera general, a todos aquellos que confiaron en mi a lo largo de estos cinco años de carrera profesional, que estuvieron atrás de mi para que no cayera, y que me brindaron el apoyo necesario para lograr la consecución de este paso en mi camino profesional.

Gracias a mi familia que, a pesar de la lejanía, no dejaron de brindarme apoyo, ánimos, consuelo y palabras de aliento.

Gracias Luis Enrique, porque tus palabras, siempre sinceras, me impulsaron y alentaron durante todo el camino para seguir siempre hacia adelante. Porque con tu buena vibra has logrado desprender la alegría en mis momentos de tristeza.

Gracias Santos porque tus consejos, aún a pesar de tu edad, siempre han sido acertados y en el momento preciso para no caer, para retomar fuerzas y seguir con mayor ánimo en el camino. Porque con tu tenacidad me has logrado decir que las acciones dan fruto conforme la firmeza del esfuerzo realizado.

Gracias Padre porque me has marcado el camino hacia el éxito, me has sembrado los valores de la responsabilidad, dedicación, constancia y perseverancia, así como la disciplina que me han llevado a lograr la conquista de este peldaño tan importante en la escalera de mi vida. Gracias por todas aquellas palabras que has dirigido hacia mi con la finalidad de hacerme crecer.

Gracias Madre porque hace casi 23 años soportaste con mucho amor los dolores que Dios te exigió para traerme al mundo. Porque han sido casi 23 años que has estado, sin ninguna clase de titubeo, tras de mi para cuidarme, protegerme y no dejar que caiga. Porque con tu sensibilidad y amor de madre has impregnado en mi ser ese entusiasmo y dedicación con el que realizo cada una de mis acciones. Porque has sido la fuente de mis más profundos acercamientos a Dios.

Gracias a mis tíos y primos que me han apoyado durante todo el camino. Gracias por compartir alegrías, tristezas, palabras de aliento y regaños. Todo lo que ha venido de ustedes me ha ayudado a crecer como persona.

Gracias a mi asesor de tesis, el Ingeniero Germán Santos, que ha confiado en mi para llevar a cabo este último proyecto de mi carrera, por haberme dedicado el tiempo necesario para lograrlo, por haberme transmitido todos los conocimientos y actitudes necesarias para llevarlo a su fin, y sobre todo, gracias por sus consejos, porque debido a ellos he seguido el camino correcto en este proyecto.

Gracias a mis sinodales por haber considerado darme parte de su tiempo para atender este trabajo de tesis y por los consejos que me han dado, los cuales me han servido de mucho.

Gracias a los maestros que, a lo largo de la carrera, han soportado las preguntas que les hacía, brotadas del ansia de adquirir el conocimiento necesario para llevar a cabo de la mejor manera esta carrera. Gracias por su paciencia.

Gracias a mis amistades más allegadas, porque nunca faltaron sus palabras de aliento siempre que las necesitaba, por abrirme las puertas de su amistad, y sobre todo por comprenderme y apoyarme en los momentos de adversidad que he tenido.

Gracias a las familias de cada uno de esas amistades, porque gracias a su apoyo incondicional han sido de gran trascendencia en mi vida. Sobre todo gracias a esa nutrida familia que me ha abierto sus puertas de manera especial, desde la más pequeña hasta el padre de la familia, los quince miembros sin excepción. Gracias a todos ellos porque han sido un ejemplo de vida para mi.

Y sobre todo, le estoy profundamente agradecido a Dios, porque, a pesar de las múltiples dificultades que he tenido en la vida, ha sido El quien ha puesto los medios y circunstancias necesarias para que yo pise hoy los terrenos que estoy pisando; porque ha contribuido con la luz que mi camino necesitaba en los momentos de mayor oscuridad; porque me ha consolado en los momentos de mayor tristeza; porque ha sido El la inspiración de mis más grandes esfuerzos en la vida; porque me ha dado las herramientas necesaria para discernir de manera correcta al tomar decisiones.

Índice

Índice

Introducción

"Una vez empezado, lo único capaz de poner límites es la imaginación". No cabe duda que esta frase se aplica a muchas situaciones que hoy en día existen alrededor de nosotros y con las cuales interactuamos cotidianamente.

Internet es un ejemplo muy palpable de esta frase, porque cuando, en 1962, Licklider[1], con su concepto llamado "Galactic Network"[2], y Leonard Kleinrock[3], con su teoría de comunicación por paquetes, empezaron a realizar sus investigaciones en los primeros conceptos de redes de computadoras nunca imaginaron que dichos conceptos serían el principio de un proyecto[4] interminable, constantemente en crecimiento y desarrollo, ambicioso y de inmensa magnitud y utilidad para la sociedad en cualquiera de sus ámbitos.

Internet comenzó con un par de computadoras, una del tipo TX2 en Massachusetts y otra del tipo Q-32 en California, conectadas por estos dos pioneros de Internet en 1965 a través de una línea telefónica conmutada de baja velocidad. Con este acontecimiento, estos dos personajes logran obtener la primera red de área amplia y, lo más importante, logran sembrar la semilla que a la postre germinaría en un mundo interconectado por una red de computadoras llamada Internet.

Poco a poco, Internet fue creciendo y presentando avances importantes. Y gracias a esto el número de empresas e instituciones interesadas en este magno proyecto, que en un principio se veía como un proyecto experimental y de magnitudes menores, fue aumentando.

En 1969, gracias a la participación de varias empresas en el proyecto, se logra conectar 4 computadoras en red, lo cual marca el inicio tangible del mundo de Internet. Y, una vez que se logra esto, se buscó hacer crecer la red que ya se había obtenido.

En el momento en que este proyecto empieza a crecer, las personas que se encuentran inmersos en el desarrollo del mismo comienzan a darse cuenta de la necesidad de la existencia de una manera en que las computadoras se puedan comunicar entre sí, se entiendan e interpreten los 0's y 1's que se mandan de una a otra para que estas puedan trabajar en conjunto. A raíz de esta necesidad empiezan a surgir los protocolos de comunicación[5] usados en Internet.

Uno de los primeros protocolos de comunicación que surgieron para el propósito mencionado fue el protocolo TCP/IP[6], el cual, desde su implementación en 1983, es el

---

[1] J.C.R.Licklider, profesor del Massachusetts Institute of Technology en Estados Unidos. Primero que escribe, en 1962, documentos acerca del concepto de red de trabajo. Ver referencia 6.

[2] "Galactic Network". Concepto que desarrollo J.C.R.Licklider en 1962, en el cuál concibe una red interconectada globalmente a través de la cuál cada uno pudiera acceder desde cualquier lugar a datos y programas. Ver referencia 6.

[3] Leonard Kleinrock. Profesor del Massachusetts Institute of Technology. Junto con Licklider, pionero de el concepto *INTERNET*. Ver referencia 6.

[4] En un principio se veía como un proyecto para lograr una red de computadoras pequeña que ayudara a compartir algunos archivos, datos y programas entre varias personas.

[5] Los protocolos de comunicación utilizados en *Internet* tienen como misión primordial posibilitar la comunicación entre todas las computadoras conectadas dentro de *Internet*. Son aquellas maneras de enviar información a través de la red mundial o a través de una red local.

[6] Protocolo de comunicación para Internet que nació en 1974 y que se adoptó en 1983, y que hasta la fecha se sigue usando como el principal protocolo de comunicación entre dos computadoras, ya sea a través de *Internet* o de *Intranet*. Ver referencia 6.

protocolo más usado para el transporte de información a través de una red de computadoras. Poco a poco fue ganando terreno en la comunicación de paquetes en una red de computadoras, hasta que llegó a ser el más usado, y en el cual se basan la mayoría de las aplicaciones hoy en día.

Una vez logrado todo esto, empezaron a surgir programas de computadora (software) usados para comunicar dos sitios alejados en diferentes partes en el mundo a través de computadoras conectadas. Con esto se empezó a desarrollar toda una amplia gama de aplicaciones. Algunas de éstas, que surgieron en los primeros años de Internet, se siguen usando, tal es el caso de correo electrónico, el cual surgió en 1972, y hasta la fecha es uno de los servicios que se provee a través de Internet que más es usado por las personas que tienen acceso a este.

Pero así como el correo electrónico, a lo largo de la historia de Internet, que data de alrededor de 35 años, han surgido una cantidad muy grande de aplicaciones para explotar la funcionalidad que tiene Internet. Aplicaciones que van desde una simple publicación de una página web, en donde se puede colocar información de cualquier tipo, hasta aplicaciones más avanzadas como teleconferencias, en donde uno puede estar viendo una conferencia que sucede en otro lado del mundo en la comodidad de su casa, y operaciones a distancia, en donde los médicos pueden estar interviniendo quirúrgicamente algún paciente que esté en otro lado del mundo.

Todo esto, que tuvo sus comienzos con la transmisión de 0's y 1's de una computadora hacia otra buscando la sola transmisión de dichos bits, ha evolucionado de manera impresionante en tan solo 35 años, esto nos habla de que la imaginación, dentro de este contexto, es la única posible de poner límites.

Por otro lado este crecimiento desmesurado de Internet se ha reflejado en todas las direcciones, como ejemplo de esto tenemos la comunicación de grandes empresas con sus clientes a través de Internet para mostrar sus productos o simplemente para mandar información[7]. Una de las mayores preocupaciones que dichas empresas tienen es que la información que ellos clasifican como confidencial caiga en personas que no deban tener acceso a dicha información. En la medida en que la información mandada, o bien la que se encuentra almacenada en las computadoras de dichas empresas, aumenta su grado de confidencialidad, en esa misma medida aumenta el deseo de protegerla de personajes o empresas competidoras que puedan dañar o puedan hacer uso indebido de dicha información, lo cual podría causar efectos graves en la compañía que es dueña de dicha información.

Este crecimiento ha traído la necesidad de almacenar grandes cantidades de información, sea o no confidencial, dentro de las computadoras, algo que ha traído la preocupación de parte de aquellas personas dueñas de dicha información por protegerla. Protegerla de aquellas personas, en muchas ocasiones con malas intenciones, que tratan de acceder a dicha información sin tener los permisos necesarios para llevar a cabo dicha operación. Estos son los llamados 'hackers'[8] o piratas de Internet.

---

[7] Información de cualquier índole, ya sea desde un simple mensaje, hasta información clasificada como secreta.

[8] Aquella persona que se dedica a entrar a sistemas burlando las medidas de seguridad que se encuentran implementadas en dicho sistema. En el mundo de *Internet*, este tipo de personas se clasifican de diferentes maneras:

Debido a este tipo de situaciones, son muchas las herramientas[9] que han surgido para evitar la intrusión de este tipo de personajes a los sistemas y proteger la información que en los mismos esté almacenada. Ya sea firewalls[10], antivirus[11], software anti-hackers[12], NIDS(Network Intrusion Detection Software)[13], entre otros. Así como hay herramientas de software para aumentar la protección en las computadoras, hay técnicas y medidas de seguridad aplicadas en el uso de los sistemas operativos para incrementar un poco más la seguridad en el mismo.

Una de las herramientas más utilizadas en la seguridad de las redes de computadoras son los NIDS, los cuales, debido a su gran funcionalidad, son muy útiles para la protección de toda una red de computadoras contra ataques informáticos[14] dirigidos hacia la red.

Uno de los sistemas que más es usado dentro de los NIDS, en el mundo de Internet, es Snort[15]. Este sistema provee una gran funcionalidad dentro de la protección de la red de computadoras, ya que es muy fácil adaptarlo a las demandas de seguridad que nuestra red exige. Básicamente este programa analiza todos los paquetes que ingresan o salen de la red, detectando aquellos que puedan resultar ser dañinos para la misma y genera acciones relacionados con dichos paquetes, ya sea no permitir su paso o generación de alertas y registro de los paquetes.

Una desventaja que trae consigo el sistema Snort es que no tiene una interfaz de usuario que le permita al administrador de la red ver en tiempo real los resultados que el sistema arroja al analizar el tráfico en la red. Este tipo de interfaz permitiría al administrador de la red estar viendo los paquetes que circulan por esta última, así como las posibles alertas generadas por dichos paquetes en el momento en que ocurren.

Hacker. Aquella persona que entra a los sistemas sin tener malas intenciones de dañarlo o de robar información confidencial, es decir, solamente entra con la intención de divertirse.

Cracker. Aquella persona que entra a los sistemas con el objetivo de dañarlo o de adquirir información a la cuál no pueda tener acceso.

Phreaker. Aquel que se dedica a burlar la seguridad en sistemas que tengan relación con compañías telefónicas.

Cualquiera que sea su nombre, este tipo de personas se dedican, o por lo menos tienen el conocimiento para hacerlo, a burlar las medidas de seguridad de los sistemas para entrar a los mismos.

También son llamados "Piratas de *Internet*". Para mayor información ver referencia 7.

[9] Generalmente software que se instala en las computadoras, y que tiene la finalidad de proporcionarle mayor protección a la información que allí se encuentra.

[10] Sistema avanzado de seguridad que impide a personas no autorizadas el acceso al sistema. En este trabajo lo manejaremos con el nombre de 'cortafuegos'. Para mayor información ver referencia 8.

[11] Software que permite detectar y desaparecer del sistema virus informáticos, los cuáles pueden resultar ser dañinos al sistema. Para mayor información ver referencia 8.

[12] Software que busca prever diferentes tipos de ataques provenientes de hackers, como por ejemplo los detectores de archivos binarios modificados para hacer algo indebido en el sistema. Para mayor información ver referencia 8.

[13] Sistema de Detección de Intrusos por sus siglas en inglés. Es software creado para proteger toda una red de computadoras de diversos tipos de ataques a la misma. Busca, mediante un filtro, detectar paquetes que se introduzcan a la red, o que salgan de la misma, que puedan resultar dañinos a la misma. En este trabajo se manejará con el nombre de 'NIDS', o bien con el nombre de 'Sistema de Detección de Intrusos'. Para mayor información ver referencia 8.

[14] Intrusiones de hackers a un sistema, ya sea para dañar el sistema o para dañar algún servicio que provea dicho sistema. Generalmente son realizados por algún, y en ocasiones varios, hacker. Para mayor información ver referencia 8.

[15] Sistema de Detección de Intrusos gratuito. Muy completo y funcional.

Así como Snort existen muchas otras herramientas que ayudan a incrementar la protección de una red de computadoras a un administrador de red.

Hoy en día la imaginación es la principal arma que tienen tanto los hacker's como las personas que se dedican a evitar las acciones de estos últimos en la lucha por lograr, por un lado burlar los sistemas de seguridad, y por otro proteger en la mayor medida posible los sistema de dichas personas.

Así, de esta manera, la imaginación es la que, poco a poco, está marcando el rumbo que está siguiendo el crecimiento de Internet.

a. La razón de este trabajo

Una de las herramientas que se usan para darle mayor protección a una red de computadoras, y que se mencionaron en el apartado anterior, es Snort, el cual es un Sistema de Detección de Intrusos que es usado mucho por los administradores de redes. Es un sistema que trabaja mediante una línea de comandos y una serie de archivos de configuración en donde se le puede indicar la manera explícita en que el sistema va a hacer su trabajo.

Como ya se mencionó, una de las desventajas que tiene este sistema es que no tiene una interfaz de usuario que le permita al administrador de red estar observando en tiempo real los datos o las alertas que Snort pueda generar. Lo que el administrador tiene que hacer para consultar dichos datos es revisar los archivos en donde Snort guarda a aquellos. Esto proceso puede causar un retraso en la detección, evasión y prevención de posibles futuros ataques. De aquí surge la necesidad de un sistema en donde se pueda observar sus salidas en tiempo real.

El motivo que impulsó al desarrollo de este trabajo es el diseño de una interfaz de usuario[16] que permita al administrador de la red interactuar con el sistema Snort desde cualquier parte del mundo a través de Internet para tener acceso a sus archivos de configuración y a los archivos de salida de datos generados, para poder administrarlo de manera remota e indicarle las acciones que el sistema debe seguir en su funcionamiento. Esto permitirá al administrador de la red tomar medidas importantes en contra de los ataques informáticos que la misma red pueda estar sufriendo, o prevenir los posibles ataques futuros; y todo esto sin estar presente en la red de computadoras en donde se encuentra instalado el sistema Snort.

Este sistema permitirá al administrador ver las salidas, alertas y resultados arrojados por Snort desde alguna otra computadora que no sea la computadora en que está instalado el sistema Snort. Así mismo permitirá la configuración y manipulación del funcionamiento del sistema.

Esto resultará muy conveniente para el administrador de la red debido a que podrá realizar algunas de las tareas de la administración de manera remota. Así mismo

[16] Interfaz visual con el cuál un usuario puede interactuar con el sistema o con otro sistema.

tendrá la capacidad de recibir la información que el sistema Snort genere en tiempo real y de manera remota, y con esto estar enterado si la red sufre de algún ataque en el momento en que es perpetuado, capacidad que le permitirá un tiempo de respuesta más corto, lo cuál puede resultar crucial en un ataque informático importante.

b. Objetivos

Diseñar todo el sistema que trabaje en compañía con Snort para que permita lo siguiente:

- Visualizar las salidas, alertas y datos generados por Snort en tiempo real.
- Configurar[17] al sistema Snort. Esto implica poder modificar todos y cada uno de los archivos de configuración.
- Administrar[18] el sistema Snort. Esto es, poder indicarle que inicie y se detenga cuando el usuario (administrador del sistema Snort, el cual, generalmente, suele ser el administrador de la red) se lo indique.
- Ser capaz de ejecutar comandos específicos para realizar ciertas tareas en el servidor para ayudar a la manipulación del sistema Snort.

Todo lo anterior podrá ser realizado a través de una interfaz gráfica de usuario, la cual podrá trabajar tanto de manera remota, es decir desde una computadora que no sea en la que esta instalado el sistema Snort, como de manera local, es decir en la misma computadora.

Lo anterior para que el administrador tenga una herramienta más para trabajar mejor con el sistema Snort.

Todo el diseño estará pensado para su posterior implementación.

[17] Referente a sus archivos de configuración
[18] Referente a manipular su funcionamiento.

Capítulo 1

Seguridad en redes de computadoras

Objetivo:

Establecer algunos conceptos importantes en el ámbito de la seguridad en redes de computadoras que se necesitarán a lo largo de este trabajo.

"El único momento en que una computadora esta por completo segura[1] es cuando está apagada y guardada en su caja". Esta frase nos indica un objetivo inherente del ser humano en relación a las computadoras, pero que resulta casi imposible llevarlo a la práctica porque implicaría una contradicción, ya que si uno tiene una computadora no es para tenerla guardada en una caja, pero por otro lado uno quiere que esté lo más segura posible.

a. Seguridad Informática

Hoy en día, cuando uno escucha la palabra seguridad puede pensar en muchas acepciones. Seguridad en un banco, seguridad en la casa, medidas de seguridad, condiciones de seguridad, etc. En fin, es tan diverso el significado de la palabra seguridad, que al escuchar dicha palabra se le torna a uno confuso interpretar el significado correcto ya que, en gran medida, la interpretación de dicho concepto depende mucho del contexto sobre el cual se este hablando.

Pues bien, la seguridad existe desde tiempos muy antiguos, en donde nuestros antepasados ya manejaban, aunque de manera instintiva, conceptos relacionados con la seguridad, tales como alertar, detectar, evitar, alarmar y reaccionar. Y dichos conceptos los aplicaban cuando recibían amenazas, ya sea de animales o de otros grupos de personas.

Así, la seguridad ha venido evolucionando a través de los años, a tal grado que en el momento en que las sociedades empezaron a vivir en familias, se implementaron medidas de seguridad para defender lo que les pertenecía a cada una de ellas, las cuales empleaban en diferentes contextos.

Pero se habla de seguridad en muchos ámbitos en nuestra sociedad, por ejemplo, desde el punto de vista legislativo, la seguridad está a cargo de los políticos, así como la legislación de los delitos que se puedan cometer. Otro ámbito es el punto de vista técnico, el cuál está a cargo la dirección de las organizaciones.

Así cuando se habla de seguridad se pueden tocar muchos ámbitos de nuestra sociedad.

Por otro lado, el concepto de seguridad, en la mayoría de sus acepciones, está relacionado con dos partes: una atacante y un defensor. En donde el atacante es el que intenta hacer daño a un defensor, que, mediante medidas de seguridad, intenta defender lo suyo. Otro concepto que se relaciona con el de seguridad es la competencia. Esto es, cuando hay competencia en un par de entes, uno busca proteger lo que le pertenece y generalmente es celoso de lo que ha producido y le ha redituado en cierta medida, esto es debido a que lo ha producido bajo cierta fórmula, la cual busca proteger; y por otro lado esta interesado en las fórmulas que le han funcionado al otro competidor. Mientras que la otra parte de la competencia hace lo propio. Esta situación provoca una actitud de protección de lo que a uno le pertenece y ha logrado con esfuerzo, lo cual nos lleva a

[1] Cuando se habla de que una computadora está segura uno se refiere a que está protegida contra ataques informáticos, acceso a información prohibida por usuarios sin privilegios, y cualquier forma de hacking en el mundo de la computación.

implementar medidas de seguridad para lograr el objetivo deseado, el cual, en este caso, se refiere al mantenimiento del estado de privado de sus datos.

Ahora bien, desde el punto de vista de la informática, es decir, todo lo referente a la computación y a la información que ésta respalda, la seguridad juega un papel sumamente importante, ya que de aquí surge el objetivo primordial de la seguridad informática: **"Mantener la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada por la computadora."**[2].

Y, dado que el manejo de la información ha crecido tan desmesuradamente como el Internet, o quizá en ciertos casos de manera más rápida, ha habido la necesidad de proteger dicha información de aquellos entes, y entiéndase entes por hackers o crackers, maliciosos, que puedan desear dañarla o robarla. Debido a esta necesidad existe la seguridad informática, concepto que surgió desde hace tiempo con el nacimiento de los grandes centros de cómputo, y que posteriormente se convirtió en una rama de la computación, conforme era más necesaria la protección de la información digital[3]. Esto debido a que cuando los grandes monstruos[4] que eran las computadoras en sus primeras generaciones pasaron a ser pequeños elementos de trabajo y se empezó a digitalizar la información se perdió la seguridad en dicha información. Algo que también ayudo a esto es el surgimiento de Internet, ya que, con el surgimiento de esta forma de conectar las computadoras, una computadora podía conectarse tanto a otras computadoras como recibir conexiones de otras, lo cual permite que el que se conecta tenga acceso a lo que existe en la computadora a la que se conecta. Esto último nació a partir del concepto de trabajo en red[5].

De esta manera el concepto de **Seguridad Informática**[6] es muy usado y socorrido por las grandes compañías que desean proteger su información contra ataques o posibles intentos de robo.

Ante todo esto, han surgido muchas herramientas para proteger la información digital. Herramientas que van desde sistemas operativos capaces de trabajar en red bajo estrictas medidas de seguridad que garantizan, hasta cierto punto, la protección de la información, hasta herramientas, algunas gratuitas y otras bajo licencia de alguna

---

[2] Obtenido del capítulo 1 de la tesis citada en la referencia 9.

[3] La información digital se refiere a cualquier tipo de información que se encuentre en alguna computadora.

[4] En un principio las computadoras, aún sin tener tanta capacidad como las computadoras de hoy en día, llegaban a ocupar pisos enteros de los edificios de las compañías que poseían dichas computadoras. Conforme pasó el tiempo, las tecnologías con que las computadoras se fueron diseñando y construyendo fueron avanzando y esto trajo como resultado que el tamaño de las computadoras se haya reducido demasiado, a tal grado que ahora haya computadoras muy pequeñas como los dispositivos llamados Palm's.

[5] El que una computadora trabaje en red significa que se pueda conectar con otras computadoras y que pueda tener acceso a ellas, así como que dichas computadoras tengan acceso a la computadora en cuestión y a la información contenida en esta última. De esta manera se puede compartir información entre las computadoras pertenecientes a la red de trabajo. Esto es muy útil cuando la tarea que se realizará por alguna computadora es muy grande, de esta forma se reparte el trabajo entre varias computadoras y resulta más eficiente.

[6] Concepto que surge ante la necesidad de la protección de la información digital, y se convierte en una rama de estudio dentro de la computación cuando el nivel de importancia de la información aumentó y se necesitó mayor protección a la misma. Mayor información en la referencia 9.

compañía, utilizadas dentro de los sistemas operativos para el mismo objetivo, la protección de la información.

b. Sistemas Operativos que trabajan en red.

Uno de los factores importantes para el desarrollo de la tecnología hoy en día es el trabajo en red, ya que permite la colaboración de varios entes en la elaboración de algún proyecto tecnológico, así como la intercomunicación entre ellos y entre sus programas para llevar a cabo el objetivo final.

Otro aspecto importante dentro del desarrollo de la tecnología son las redes de computadoras[7], ya que las tecnologías nuevas, y las que están por venir, están basadas, en gran medida en la realización de diversas tareas a distancia a través de este medio. De aquí nace la importancia de las redes de computadoras en el desarrollo de la tecnología.

Conforme el desarrollo lo exigía, las redes de computadoras fueron evolucionando[8], así como los sistemas operativos que trabajan en un ambiente de redes de computadoras.

Es importante aclarar que un sistema operativo se puede definir como **"El encargado de administrar los recursos de la computadora para sacarle el mayor provecho en beneficio del usuario. Este es capaz de soportar software para facilitar el trabajo de diversas tareas del usuario"**

Los sistemas operativos juegan un papel sumamente importante en el buen funcionamiento de una red de computadoras, ya que son los encargados de establecer la comunicación entre dos computadoras pertenecientes a dicha red a nivel lógico[9]. Esto significa que mientras las redes de computadoras se forman conectando computadoras mediante cables y otro tipo de hardware[10], los sistemas operativos son los que hacen capaces a dichas computadoras de comunicarse entre sí dentro de dicha red.

En este sentido, una red de computadoras no solamente esta formada por las máquinas, que en si no son mas que un conjunto de componentes electrónicos, si no que también se forman por los sistemas operativos que contienen estas máquinas, y que en un punto determinado son los que se encargan del buen funcionamiento e intercomunicación entre las computadoras de una red.

---

[7] Una red de computadoras es un conjunto de computadoras conectadas entre si bajo una topología para realizar una tarea entre todas las computadoras conectadas, logrando así una mayor eficiencia a la hora de realizar tareas o muy complejas o muy largas. Mayor información en la referencia 8.

[8] Fueron creando tipos de topología de conexión más eficientes, hardware de conexión con mayores capacidades, protocolos nuevos, entre otros aspectos dentro de la creación de una red de computadoras.

[9] A nivel de software, es decir, el envío y recepción de 0's y 1's de tal manera que las computadoras se entiendan lo que se están enviando unas a otras. De esta manera logran una comunicación ordenada y útil para la realización de tareas específicas.

[10] Este tipo de hardware comprende muchos aparatos, los cuáles no son tema de este trabajo, como switch, hub, router, entre otros.

En general se puede decir que un sistema operativo tiene las siguientes características: conveniencia, eficiencia, habilidad para evolucionar, manejo de la comunicación en red y soporte de software que trabaje en red.

Existen varios tipos de sistemas operativos; como ejemplo de ellos están los que no trabajan en una red de computadoras, los cuales están orientados a trabajo de escritorio; los que soportan el trabajo en una red de computadoras, los cuales también soportan el trabajo de escritorio; y los que son hechos especialmente para trabajar en una red de computadoras, los cuales tienen las funciones de red optimizadas; y, finalmente, los que son creados para soportar y optimizar las tareas de una red de computadoras con una tarea específica, los cuales son creados para realizar una tarea específica dentro de una red de computadoras.

Los sistemas operativos de red, además de soportar multitareas concurrentes y distribuidas[11], tienen las características de manejar direccionamientos de paquetes[12], manejo de protocolos[13] y administración de recursos de servidor[14], así como también incluyen una arquitectura de seguridad de acceso de usuarios[15].

Algunos de los sistemas operativos que trabajan en red, junto a una breve mención de algunas de sus características más importantes, se mencionan a continuación[16]:

- **Novell Netware**
Creado por la compañía Novell.
Arquitectura multiusuario y multitarea.
Le es posible restringir el acceso al sistema por medio de claves de usuario.
La integridad del sistema es asegurada por medio de bloqueo a directorios y archivos. Admite estaciones de trabajo que operan bajo OS/2.
El sistema de control de usuarios permite establecer horarios de conexión, así como fechas de expiración de las cuentas.
Las cuentas de usuario pueden dejar de estar accesibles temporalmente.
La duplicación de estructuras de directorios permite prevenir la pérdida de archivos y la inutilización de datos.
Permite comunicaciones a larga distancia, gracias a conexiones remotas asíncronas.

- **Windows NT/2000/XP**
Creado por la compañía Microsoft.
Capacidad controlador de dominios.
Capacidad de Trust.
Perfiles de usuarios centralizados
Replicación de directorios

[11] Pueden realizar varias tareas a la vez con un mismo procesador, o con varios procesadores, así como pueden realizar una tarea entre varias computadoras.
[12] Mandar los datos solamente a la computadora, o computadoras que lo necesiten.
[13] Son las formas en que una computadora envía la información a otra computadora para poder entender los datos que le envía.
[14] Capaz de controlar y administrar todos y cada uno de los recursos de hardware que posee la computadora para lograr un mayor beneficio y eficiencia.
[15] Generalmente llamada autentificación de usuarios.
[16] Para mayor información dirigirse a referencia 10.

Servicio de acceso remoto
Servicio para Macintosh y otras características.
En cuanto a los servicios de servidores que puede soportar existen los siguientes: servidores de base de datos, servidores de mensajería, servidores de archivos e impresión, servidores de comunicaciones y servidores WEB entre otros.

- **OS/2**

Creado por IBM.
Es multitarea, usado para aplicaciones críticas y servidores.
Es estable.
Capaz de ejecutar programas de Windows.
Escritorio cómodo para trabajar, compatibilidad con otras plataformas como Windows, es seguro para el uso en Internet.
Tiene múltiples usos como juegos, Internet, multimedia, aplicaciones de oficina, gráficos, base de datos, y otros.

- **Linux**

Es uno de los sistemas libres más robusto que existe. Se desarrollo, en sus múltiples versiones, por varias compañías de manera separada, es decir, existen tantos tipos de linux como compañías que lo desarrollan.
Entre sus principales características están las siguientes: seguro, estable, escritorio de trabajo agradable, trabajo en red seguro, robusto, multitarea, multiusuario, multiplataforma, protección de memoria entre procesos, sistema de archivos, control de tareas, gratuito, entre otras.
Su uso se extiende a muchos ámbitos: juegos, oficina, red, base de datos, Internet, intranet, gráficos, desarrollo científico, entre otros muchos.

- **Unix**

En un principio creado por varias compañías: MIT, General Electric, Bell Labs de AT&T. Posteriormente, cuando vino su auge, varias compañías empezaron a desarrollarlo y con esto vinieron las diferentes versiones de UNIX, incluyendo Linux.
Entre sus características importantes se encuentran: multiusuario, multitarea, facilidad de creación de programas, manejo dinámico de memoria, capacidad de interconexión de procesos, comunicación entre procesos, sistema jerárquico de archivos, facilidad de redireccionamiento de entradas/salidas, alto grado de portabilidad, trabajo en red, estable, seguro, confiable.
Sus usos son tan diversos como los del sistema operativo linux.

De esta manera, podemos concluir que un sistema operativo es el corazón de una computadora, así como parte sumamente importante en el funcionamiento correcto de una red de computadoras.

c. Aspectos a tomar en cuenta en la seguridad en redes de computadoras.

Existen muchos aspectos que se deben de tomar en cuenta en la cuestión de seguridad en redes de computadoras. Aspectos que van desde las cuestiones básicas

como las contraseñas para los archivos personales, hasta los aspectos avanzados como la criptografía u otro tipo de protección como cortafuegos o sistemas de detección de intrusos.

Cada uno juega un papel importante en la seguridad de la red en cuestión, ya sea en mayor o menor medida, pero todos son importantes dentro de una red segura.

Son importantes los aspectos que se puedan tomar en cuenta respecto a proteger una red mediante software. Pero un aspecto de igual importancia es el de la cultura de la seguridad. Esto nos habla de la manera en que un usuario de una red de computadoras toma sus precauciones para que sus archivos sean seguros y con esto contribuya un poco, y en ocasiones en gran medida, a la seguridad de dicha red.

Algunos de los aspectos importantes en la seguridad en redes de computadoras son los siguientes:

- **Cultura de la seguridad.**
Es importante que los usuarios de la red de computadoras tengan claro que el primer eslabón de la seguridad en ésta última son ellos mismos. Esto se debe a que si algún usuario no tiene la costumbre de proteger sus archivos y guardarlos en los lugares adecuados para cada archivo, podría generar problemas de seguridad en el sistema operativo, con lo cual podría llegar a hacerlo vulnerable a ataques a la computadora que se encuentra usando o inclusive a la red de computadoras en donde se encuentra.
Es por esta razón que la cultura de la seguridad es importantísima. No sirve de nada que un administrador[17] de redes de computadoras proteja la red de manera muy detallada si algún usuario provoca, mediante alguna transacción o algún movimiento dentro de su cuenta, alguna vulnerabilidad en el sistema protegido o en la red protegida.

- **Contraseñas.**
Es importante que cada usuario en la red de computadoras tenga su propia contraseña, así como también es de igual o mayor importancia que dicha contraseña sea difícil de descifrar, es decir que contenga dígitos, caracteres y símbolos. Una contraseña fácil de descifrar puede ser la causa de una intrusión no deseada a la red de computadoras o a la computadora donde se encuentra dicha contraseña. Es importante que el administrador de la red recomiende y observe que la contraseña usada por los usuarios cumpla con las características mínimas de seguridad.
Todo esto para evitar intrusiones fáciles no deseadas a la red protegida.

- **Revisión constante de los programas ejecutables.**
Uno de los puntos vulnerables de un sistema operativo es un programa ejecutable modificado, el cuál puede generar "puertas traseras"[18] en el sistema

[17] Es el encargado de mantener el buen funcionamiento de una red de computadoras.
[18] En inglés se llaman "backdoors" (puertas traseras), las cuáles son provocadas por programas modificados. Cuando uno ejecuta dichos programas, estos abren una conexión hacia el exterior de la computadora sin que el usuario que lo ejecuta se de cuenta de esto. Esto provoca que alguien fuera de la computadora pueda establecer una conexión sin que el usuario dentro de la computadora en cuestión se de

operativo, con lo cuál lo deja abierto a cualquiera que quiera entrar a hacer lo que él desee.
Es recomendable que el administrador de la red de computadoras lleve a cabo este tipo de chequeos cada cierto tiempo, dependiendo del uso y tráfico de la red.

- Métodos de autentificación.
Colocar métodos de autentificación en el momento de ingresar un usuario, para que estos solo puedan ingresar a través de una contraseña. De otra forma cualquier usuario podrá ingresar al sistema sin ningún tipo de restricción.
Esto evita que algún intruso tenga las puertas abiertas con solo averiguar cual de los usuarios del sistema es el que no cuenta con una contraseña de acceso al sistema[19].
Uno como administrador de redes se puede evitar muchos problemas si implementa esta medida de seguridad.
Existen varias maneras de implementar métodos de autenticación, y dichas maneras generalmente vienen algunas en el conjunto variado de sistemas operativos, así como en sus diferentes versiones. Aparte de las herramientas de autenticación que te provee el sistema operativo, en Internet, o mediante las compañías desarrolladoras de este tipo de herramientas, se pueden adquirir otras para que los métodos de autenticación sean más completos o inclusive más complejos, de tal manera que para un intruso le sea más difícil evadir esa parte de la seguridad en los sistemas.

- Antivirus
Es un método muy socorrido, por los administradores de red, para evitar que las computadoras adquieran algún programa que pueda ser dañino para la misma computadora, o inclusive para la red.
Se sabe que la cantidad de virus informáticos[20] desarrollados por los hackers son muchísimos, y dichos virus, en su mayoría se transmiten por medio de Internet, a través de la transición de programas de una computadora a otra o por medio del mail. Y, ante esta situación, lo más recomendable es que uno proteja la computadora con este tipo de herramientas.
Existen muchas maneras de que una computadora adquiera un virus informático.

- Cortafuegos.
Es una manera más compleja que las anteriores de proteger una red de computadoras, ya que este tipo de software, controla el paso de paquetes de datos[21] a la red basándose en una serie de reglas indicadas por el administrador del cortafuegos.
La manera en que funciona este tipo de software es mediante reglas, las cuales uno como administrador de la red se las da, y el software, de acuerdo a dichas reglas, deja pasar los paquetes o los detiene en la entrada a la red.

---

cuenta, lo cuál podría causar problemas mayúsculos cuando dicha conexión se usa para propósitos maliciosos.

[19] Es una palabra clave asignada al usuario, o elegida por él mismo, para ingresar al sistema.

[20] Programa capaz de dañar el funcionamiento de una computadora, e inclusive, en ocasiones, es capaz de perjudicar el buen funcionamiento de la red.

[21] Conjunto de datos que se transmiten a través de una red. Los cuáles van dirigidos a las computadoras, y éstas se encargan de interpretarlos.

Hay algunos tipos de cortafuegos muy completos que registran los movimientos que tiene la red en cuestión de paquetes, otros que realizan alguna acción en contra del origen o en contra del paquete dañino.
En fin, la variedad de este tipo de software es muy amplia, uno elige el que se le haga más conveniente de acuerdo a sus recursos tanto económicos como de conocimientos, así como de acuerdo a sus necesidades de protección de datos.
Muchos son gratuitos, algunos otros, muy completos, cuestan, y el precio puede variar mucho, dependiendo del fabricante y de las características que ofrezca el software que se quiere adquirir.

- Sistemas de detección de intrusos.
Es otra forma de proteger una red. Este tipo de software solamente, en la mayoría de los casos, detecta los paquetes y realiza algo con ese paquete de acuerdo a la regla que el administrador colocó en la configuración del sistema que se acople al paquete en cuestión.
La manera de trabajar de este tipo de software es similar a los cortafuegos. Lo hacen mediante reglas que el administrador declara, dichas reglas pueden decirle al sistema de detección de intrusos que realice alguna acción en contra del paquete o en contra de la dirección IP de origen o alguna otra acción parecida.
Una de las ventajas de estos sistemas es que son sencillos de usar y son muy útiles para detectar diferentes ataques hacia la red.
El inconveniente que tienen estos sistemas es que no pueden detectar ataques dentro de la misma red de computadoras, es decir, no pueden detectar, en su mayoría, ataques generados por algún miembro de la red.

- Criptografía.
Es una manera fácil de proteger los archivos que uno genera dentro de un sistema.
Este método consiste en tomar un archivo, el que se quiera proteger, tomar byte por byte, y aplicarle algún método de transformación, de tal manera que los bytes queden desordenados o codificados[22]. Esto para que no se tenga acceso a la información de manera directa, es decir, que sea necesario decodificar el archivo resultante para poder acceder nuevamente a la información.
Así mismo, debe existir un método de decodificación para regresar el archivo resultante a su estado original, de tal manera que no se quede en su estado codificado y se pueda volver a leer.
Existen muchos métodos de codificación de archivos, algunos simples y otros complejos.
Este método se usa también para la transmisión de datos a través de Internet o a través de una intranet.

Así como los aspectos mencionados arriba, existen otros aspectos que se tienen que tomar en cuenta a la hora de implementar la seguridad en una red de computadoras. Todo esto para un administrador de redes puede llevarle algunos días, o en ocasiones más, de tiempo, pero todo se hace con el fin de tener protegida lo más que se pueda los datos que la organización desea proteger su acceso de las personas ajenas a ella.

[22] Método en el cuál los bytes de los archivos quedan con una estructura diferente a la original, de tal manera, que solamente aquella persona que los colocó bajo esa estructura sea capaz de volverlos a colocar de nuevo bajo su estructura original para que se pueda volver a leer el archivo. Para mayor información dirigirse a la referencia 11.

d. Métodos que ayudan a mantener la seguridad en redes.

Hoy en día existen muchos métodos que ayudan a un administrador a mantener la seguridad de los recursos informáticos en una red de computadoras. Algunos son caros, otros son gratuitos; algunos son difíciles de mantener, otros son sólo cuestión de tener cultura de seguridad.

Algunos de los métodos más usados para lograr un mayor nivel de seguridad son los siguientes:

i.Detección de intrusos[23]

Por intrusión se entiende acceder, o manipular, a cierta información a la que no se puede tener acceso, o hacer que un sistema no funcione de forma segura. Hoy en día existen métodos que ayudan a controlar el acceso hacia una red desde algún lugar externo a la misma. Pero este tipo de métodos pueden ser vulnerables, así que para detectar algún ataque o intrusión a la red se utiliza el método llamado 'Detección de intrusos'.

Para detectar las características que detallan alguna intrusión al sistema, existen varias metodologías. Algunas son la búsqueda, en los archivos de bitácoras del sistema, de las posibles huellas que haya dejado el intruso cuando haya estado en el sistema en cuestión. Esta técnica consta de una serie de pasos, los cuáles consisten en revisar varios tipos de archivos en el sistema que guardan cada uno de los movimientos que se realizan en el mismo. Archivos tales como los llamados 'archivos log', los cuáles registran la mayoría de los movimientos de un sistema, tanto los archivos de log que registran las conexiones como los que registran los movimientos del sistema.

Otros archivos que hay que revisar con sumo detalle son los archivos ocultos, es decir, los que empiezan su nombre con un punto '.', ya que éstos pueden ser usados para esconder herramientas para violar la seguridad del sistema. Otros archivos importantes a revisar con sumo detalle son los archivos SET-UID. En fin, estos y otros archivos, que se detallarán en la sección 3, son los que hay que revisar después de una intrusión no deseada.

Así como existe este tipo de metodologías a seguir, también existe software que ayuda a realizar esta ardua tarea. Este tipo de software se verá con más detalle en la siguiente sección.

ii.Criptografía

La criptografía, en el mundo de la informática tiene varios significados, aunque todos ellos muy similares:

- Técnicas de escrituras tales que la información esté oculta de intrusos no autorizados
- Ciencia que estudia los métodos y procedimientos, mediante algoritmos matemáticos, para modificar los datos de tal manera que solamente las personas que tengan llave adecuada puedan tener acceso a la versión original de los mismos (confidencialidad) y asegurar que estos datos no fueren modificados entre el remitente y el destinatario (integridad)

[23] Acción de localizar a las personas que se quieren conectar al sistema y que son ajenas al mismo.

Estas y otras son las definiciones que se le dan al concepto de criptografía. Pero, como podemos observar, son definiciones similares, ya que están orientadas o hacia un objetivo similar, ocultar la información que se maneja para que personas ajenas a la misma no tengan acceso a ella.

Este es otro de los métodos que los usuarios en Internet, así como en redes de computadoras de alguna compañía, así como administradores de alguna red de computadoras usan para proteger su información de los intrusos o de las personas que quieren acceder a esta sin tener permisos de tal acción.

En la medida en que se tiene información más importante que proteger contra algún ataque o intrusión no deseada, se encuentran métodos de encriptación de la información más complejos, esto es porque los intrusos o crackers han hecho y seguirán haciendo todo lo humanamente posible por burlar[24] los métodos de encriptación ya existentes.

Existen varias metodologías de encriptación de información, y dentro de dichas metodologías existen muchas variantes para realizar la encriptación.

Y ya que, por un lado, existe un gran interés por la protección de información confidencial de parte de los propietarios de dicha información, y, por otro lado, existen personas con malas intenciones que buscan acceder a ésta última por cualquier medio, surge una especie de competencia entre los expertos en criptografía y desarrollo de métodos criptográficos para ocultar la información y los hackers, la cual trae consigo beneficios como el surgimiento de métodos criptográficos más complejos y eficientes

iii.Claves de usuario

Es un método sencillo para proteger un poco más los sistemas de cómputo y la información guardada en ellos.

Y, aunque parezca sencillo, este método es sumamente importante que se lleve a cabo de la mejor manera posible para dificultar todavía más a un intruso la realización de su ataque.

Este método tiene su complicación, la cual radica en que las claves tienen que contener caracteres de todo tipo, es decir, alfanuméricos, y símbolos también. Esto para que el intruso batalle más cuando quiera descifrar alguna clave para entrar al sistema. Otra cuestión que tiene que tener este método, es que la manera en que se colocan los caracteres en la palabra clave no deben llevar algún orden ni tener algún significado, es decir, solamente elegir algunos caracteres y acomodarlos de la manera más 'desordenada'[25] posible para asegurar una clave difícil de descifrar. Las últimas dos, aunadas a algunas otras, son recomendaciones que se le dan al usuario, por parte del administrador de la red, para evitar una posible intrusión con alguna clave fácil de descifrar. Por último, en este método se recomienda que al usuario que elija más de 6, u 8 en muchas ocasiones, caracteres o símbolos para formar su contraseña.

En este rubro hay un detalle que hace difícil la implementación de dicho método, el usuario no está acostumbrado a manejar caracteres que no sean los del alfabeto, y mucho menos está acostumbrado a manejarlos sin que tengan una secuencia lógica, y es por esto que, aunque es de suma importancia que este método de protección de información se lleve a cabo de la mejor manera posible,

[24] Evadirlos o lograr descifrar los métodos de encriptación para obtener la información cifrada.

[25] Refiérase a la manera en que se colocan los caracteres elegidos en una contraseña. En muchas ocasiones el orden en que se colocan es al azar, para que no sea tan fácil de descifrarla por personas ajenas a dicha contraseña.

es difícil su correcta implementación ya que no depende por completo del administrador de la red. En gran medida existe dicha dificultad en la implementación de este método porque la mayoría de los usuarios no tienen una cultura[26] adecuada acerca de la seguridad informática.
Y este problema, la falta de cultura de seguridad, es el que viene a hacer que los métodos de aseguramiento de la información, en algunas ocasiones, se vuelvan fácilmente vulnerables.
En este rubro, si los usuarios no tienen una buena cultura de la seguridad informática, el administrador de la red se debe preocupar, en cierta medida, de promoverla en ellos, ya que esto contribuirá un poco más a la protección del sistema.

iv.Cortafuegos[27] (Firewalls)

Existe otro tipo de software que ayuda a la protección de los datos que se encuentran en alguna red de computadoras, son los llamados cortafuegos, los cuales trabajan por medio de políticas de acceso dictadas por reglas escritas por el administrador del cortafuegos, que generalmente se trata de la misma persona que administra la red donde se encuentra instalado dicho software.
Una de las definiciones que se le ha dado a este tipo de sistemas es la siguiente: **"sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet"**.
Dicho software determina, mediante las políticas de acceso antes mencionadas, cuales de los servicios de red pueden ser usados dentro de esta por los usuarios que se encuentran fuera, es decir, que servicios tienen acceso desde el exterior de la red de computadoras para su uso.
Para que este método sea efectivo, el cortafuegos deberá estar instalado en la puerta de entrada y salida de la red hacia Internet. Esto para que tanto los datos de entrada (los que vienen de Internet hacia la red) como los datos de salida (los que los usuarios internos de la red envían hacia Internet) pasen por el cortafuegos, y a partir de las reglas definidas en éste, la información pase o se detenga hacia afuera o hacia adentro de la red de computadoras en cuestión.
Esto evita que información no deseada entre o salga de la red.
Algunas de las ventajas de este tipo de software son las siguientes:
- Permite al administrador de la red mantener al margen a los usuarios no autorizados que vengan fuera de la red. Esto permite prohibir la entrada o salida de paquetes de datos que puedan hacer vulnerable nuestra red a ataques informáticos desde su exterior. Es por este motivo que es importante que el administrador de la red tenga conocimiento de las características de la mayor

[26] Cultura acerca de la seguridad informática en un usuario se refiere a que dicho usuario se preocupe por contribuir a la protección de su información. Dicha preocupación surge a partir de dos cuestiones: el usuario se da cuenta de la importancia de proteger el sistema de ataques externos al mismo, y el usuario tiene el interés de mantener en la confidencialidad su información. Esta cultura se ve reflejada en sencillas acciones como elegir una buena contraseña, es decir, difícil de descifrar y con las características ya mencionadas, aplicar métodos de encriptación a la información personal, asignar adecuadamente los permisos necesarios a cada uno de los archivos pertenecientes a dicho usuario, entre otras muchas. Como se puede observar son cuestiones simples, pero desgraciadamente la mayoría de los usuario de una computadora no se preocupa por eso, lo cuál le acarrea más trabajo al administrador de la red ya que este tiene que implementar otros métodos para suplir a los recién mencionados para darle mayor protección al sistema y a la información de los usuarios.

[27] Software que coloca restricciones en la entrada y salida de paquetes de datos en una red de computadoras o en un equipo específico. Para mayor información dirigirse a la referencia 8.

cantidad de ataques por Internet, para que le indique al cortafuegos que los detecte y no los deje pasar.
- Ofrece un punto en donde la seguridad puede estar en constante monitoreo, y, en caso de que aparezca una actividad sospechosa dentro del tráfico de la red, el cortafuegos puede realizar diferentes acciones en contra de dicha actividad, como por ejemplo generar algún tipo de alarma. Esto le sirve al administrador de red para darse cuenta en que momento vino el ataque desde fuera de la red, ya que el cortafuegos no solamente puede generar una alarma, sino que también registra dichos movimientos sospechosos en una bitácora para su posterior utilización.
- Otro de las utilidades que el cortafuegos ofrece es el registro de la actividad del uso de Internet. Esto es debido a que el firewall, en caso de que este instalado en la antesala a Internet dentro de la compañía, es el punto de salida de una red hacia Internet, por lo que puede darse cuenta cuáles y en cuántas ocasiones los usuarios de la red visitan una página. Esto es muy útil porque le dice al administrador las estadísticas sobre las páginas que los usuarios de la red visitan.
- Dado el punto anterior, los cortafuegos tienen también la capacidad de bloquear el acceso a ciertas páginas, o bloquear los datos que son enviados desde ciertas páginas hacia algún usuario de la red. Esto permite controlar el flujo de datos restringiendo las páginas que se acceden en Internet.
- Otra de las ventajas del cortafuegos es que tiene la capacidad de bloquear[28] puertos[29] en una computadora. Esto consiste en no permitir la entrada a la computadora, o a una red, de información de cualquier índole. Y, puesto que los ataques generalmente se llevan a cabo por puertos específicos, con esto se le da mayor seguridad a la computadora.
Como se puede observar, este tipo de software es muy útil en la búsqueda de la seguridad de una red de computadoras. Pero, aunque sus ventajas son muy útiles y atractivas, un cortafuegos no garantiza por completo la seguridad de la red, debido a que si la red tiene otra salida a Internet no protegida, la red queda en estado vulnerable a ataques por dicha salida.

v.Otros

Además de los ya mencionados métodos de protección de la información existen otros métodos que se explican de manera breve a continuación:
1.Programas seguros en el sistema. Los programas que se desarrollen dentro del sistema, o fuera del mismo, y que se guarden en el sistema deben de ser seguros, es decir, no deben de causar, en su funcionamiento, algún problema relacionado con la memoria del sistema, el sistema de archivos o con la apertura de sockets que no sean cerrados. Esto para evitar que se generen vulnerabilidades en el sistema.
2.Antivirus. Esto con la finalidad de estar detectando cada cierto tiempo, e inclusive en muchas ocasiones constantemente, la presencia de virus en el sistema que puedan causar alguna falla o alguna 'puerta trasera de entrada' en el sistema.

[28] No permitir su uso, tanto en la entrada como en la salida de paquetes de datos.
[29] Son accesos, o en su defecto salidas, que el sistema operativo implementa para que el usuario o el software de dicha computadora pueda tener comunicación con el exterior.

3.Auditoría[30] del sistema. Es recomendable el estar auditando el sistema cada cierto tiempo. Las auditorías al sistema consisten en verificar que dentro del mismo no haya archivos maliciosos, verificar las operaciones que se han registrado en el sistema de 'log', ya sea de mensajes, del sistema, de fallos, o de todo tipo de registro en el sistema, entre otros.

4.Copias de seguridad[31]. Cuando un intruso accede a una red sin permiso puede hacer casi cualquier cosa dentro de ella, inclusive modificar o borrar la información. Es debido a esta razón que es importante tener siempre un respaldo de la información importante por si dicho intruso decide borrar la información habida en la computadora en cuestión. Para esto existen varios métodos para la realización de copias de seguridad, algunos de dichos métodos te los ofrece el mismo sistema operativo y otros te los ofrece algunos tipos de software en la red, en la mayoría de los mismos son gratuitos. Este método entra a formar parte de la cultura de seguridad que los usuarios deben de adquirir.

Este método, en gran medida, contribuye a la recuperación de la información original, en caso de que esta última haya sido modificada o borrada. Y, aunque es muy útil este método, en muchas ocasiones no se puede recuperar toda la información perdida. Esto es porque cuando se hace el respaldo queda guardada la información que existía en dicho momento, pero si la información se está actualizando constantemente, el estado de la misma cambia. Y, en un momento dado, si la información se pierde, se puede recuperar solamente lo que se había respaldado. Esto nos lleva a establecer ciertas políticas de tiempos para el respaldo de la información.

5.Autenticación de usuarios[32]. Esto va muy de la mano con el punto 'Claves de usuario' explicado anteriormente. Existen varios métodos de autenticación de usuario, algunos de los cuales te los proporciona el mismo sistema operativo, mientras que otros, quizá más complejos, te los proporcionan algunas compañías mediante su software.

Estos son algunos de los métodos que los administradores de redes utilizan para incrementar un poco la seguridad en redes. Existen muchos otros métodos utilizados en este ámbito como las políticas de seguridad que se definen dentro de un ambiente de trabajo o en una compañía para incrementar un poco más la seguridad en sus datos privados.

A pesar de la existencia de todos estos métodos de seguridad de un sistema o de alguna red, como se mencionó en el principio de este capítulo, la total seguridad en una red es casi imposible de alcanzar.

Se dice que la única manera de alcanzar la plena seguridad en la información que se encuentren dentro de alguna computadora es teniendo a esta última apagada. Esto es porque, aún sin tenerla conectada a la red, el sistema operativo puede generar un error y borrar la información contenida en él. Y cuando una computadora está conectada a algún tipo de red, esta es propensa a que desde alguna otra computadora conectada, de manera directa o indirecta a la misma red puede tener acceso a dicha computadora. Es

[30] Revisión que se da a la computadora en todos los componentes de la misma. Generalmente, bajo este contexto, se realiza con la finalidad de mantenerlo segura.

[31] Copias que se le hace a varios, o en ocasiones a todos los archivos, de los archivos del sistema, con la finalidad de tener un respaldo en caso de que suceda algo con los originales.

[32] Es la manera en que el sistema operativo comprueba si el usuario puede o no entrar al sistema.

debido a esta razón que la posibilidad de un ataque a la información de una computadora siempre está vigente. Y esta posibilidad se incrementa de manera proporcional a la importancia de dicha información. Todo esto porque las personas interesadas en tu información buscan la manera de burlar tus medidas de seguridad para lograr sus objetivos.

Es por eso que: "Ningún sistema de seguridad de redes de computadoras es suficiente para alcanzar la absoluta protección de la información contenida en la misma".

e. Herramientas[33] existentes.

Existe una gran variedad de herramientas para cada uno de los métodos utilizados para el incremento de la seguridad en la información.

La elección, tanto de los métodos utilizados como de las herramientas que llevarán a cabo la implementación de dichos métodos, depende de dos factores, los cuáles se pueden resumir en dos preguntas:

- **¿Qué se quiere proteger?**
  Ya que es muy diferente proteger información personal de tipo no muy importante y proteger información altamente confidencial de algún gobierno.
  Para la primera podría bastar con una simple copia de seguridad, pero para la segunda se tendrían que implementar métodos que garanticen altos grados de protección de la información.

- **¿De quién se quieren proteger?**
  Uno puede protegerse de muchas cosas, como algún ataque de una o varias personas, de errores lógicos en el sistema operativo, o catástrofes ya sea a nivel sistema operativo o a nivel hardware.

Algunas herramientas, de acuerdo al método de protección, se mencionan a continuación[34]:

- **Detección de intrusos.**
  - Snort
  - Patrol
  - Tivoli
  - HP Openview
  - AID
  - NetRanger – CISCO Systems
  - Otros

[33] Ayuda, ya sea de software o hardware, para la realización de alguna tarea. En nuestro contexto, dicha tarea es la obtención de la seguridad de la información.

[34] Cada una de las herramientas mencionadas a continuación son tipos de software disponibles en Internet o en compañías que lo venden. Existen más, aunque las mencionadas son las más usadas o las más importantes. No se explican en este trabajo ya que no es intención de él mismo.

- **Criptografía**
  - Clave Pública
  - Clave Privada
  - PGP – Pretty Good Privacy
  - SSH (Secure Shell)
  - Otros

- **Autenticación y claves de usuario.**
  - Kerberos
  - Access Tokens (Windows NT)
  - Security IDS (Windows NT)
  - EAP (Extensible Authentication Protocol)
  - MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)
  - Otros

- **Cortafuegos.**
  - MindSoft Firewall
  - Norton Personal Firewall 2003
  - Norton Internet Security 2003
  - Sygate Personal Firewall Pro 5.0
  - McAfee Firewall 4.0
  - Tiny Personal Firewall
  - Otros

- **Otros.**
  - McAfee Antivirus
  - Symantec Antivirus
  - Panda Antivirus
  - E-Trust Antivirus
  - Norton Antivirus
  - Auditoria de sistemas
    - Tripwire
    - SARA
    - Nlog
    - Symon
    - WebTrends LogAnalyzer
  - Copias de seguridad
    - Acronis True Image
    - NTI Backup
    - StuffIt
    - Handy Backup
    - Simple Backup
  - Análisis de tráfico en la red
    - Nessus
    - Ethereal
    - Snort
    - Netcat
    - TCPDump/WinDump

Como se puede observar el administrador tiene un conjunto de herramientas muy amplio para tratar de darle mayor seguridad a los datos privados que se alojan en la red que está administrando.

Cada una de las herramientas tiene su propia funcionalidad y se especializan en alguna tarea de la administración de la red. Es importante mencionar que ninguna herramienta, por si sola, tiene la capacidad de proporcionar toda la funcionalidad de la administración de redes. Es debido a esto que usualmente se instalan varias herramientas dentro de un sistema, e inclusive dentro de toda la red en cuestión.

La elección de cada una de las herramientas depende del usuario, ya sea el administrador de la red o un usuario normal de la misma, que la elige, de la funcionalidad de la misma y de los recursos tanto económicos como de hardware con los que se cuenta en dicho momento. Cada uno de estos factores ayuda a definir el grado de seguridad que puede tener una red.

Algunas de las herramientas mencionadas, son gratuitas. Y esto no significa que sean de baja calidad, o estén incompletas, pero generalmente las herramientas no gratuitas tienen soporte técnico, algo que ayuda mucho al administrador de la red cuando dicho software falla o genera algo extraño en el sistema. Este factor es muy importante, debido a que si alguna herramienta falla, uno como usuario puede pedir información acerca de dicha falla a la empresa que desarrolló el software.

La finalidad es asegurar lo más que se pueda nuestra red, pues entonces, la herramientas están en la puerta de Internet.

Capítulo 2

Detección de Intrusos

Objetivo:

Establecer el fundamento teórico del área de 'Detección de Intrusos', área sobre la que se basa gran parte de este trabajo. Acerca del funcionamiento, ventajas y desventajas, tipos y software existente de Sistema de Detección de Intrusos.

Como se ha dicho antes, la seguridad plena en un sistema de cómputo[1] solamente se puede alcanzar desconectando de la red electrica a este último y no usándolo. Pero esto implicaría que dejara de realizar las funciones de sistema de cómputo, por lo cual dejaría de ser útil al usuario final.

La posibilidad de que el sistema de cómputo sea atacado[2] o dañado se vuelve mayor cuando este último esta conectado a Internet, ya que cualquier otra computadora en Internet puede tener acceso a este sistema de cómputo.

Hoy en día, en definitiva, la seguridad en Internet[3] es muy importante para empresas e instituciones de gran magnitud. Y, así como existe una gran variedad de métodos para alcanzar una seguridad aceptable en los sistemas de cómputo, dentro de dichos métodos se encuentra la detección de intrusos, la cual esta catalogada como una importante metodología dentro de este gran rubro.

La detección de intrusos es la actividad que permite conocer en tiempo real[4] si algún invitado no deseado[5] está tratando de entrar a la red de computadoras que administramos a realizar actividades que puedan perjudicar a la misma[6].

Hoy en día se sabe que la información se tiende a almacenar de manera completa en formato digital[7]. Debido a esto es mucho más fácil acceder a esta por medio de redes de computadoras, ya que estas últimas nos permiten el paso de datos[8] entre computadoras que se encuentren a cualquier distancia. Dicha información puede ser de diversa índole: financiera, gubernamental, militar, industrial, comercial, personal, entre otros. Y, por desgracia, existen personas[9] malintencionadas, y sin ética, que buscan obtenerla y usarla para su beneficio, y en ocasiones hasta destruirla.

Debido a este tipo de personas, las cuales buscan por cualquier medio adueñarse de la información clasificada, empezó a crecer el estudio y desarrollo de métodos para incrementar la seguridad en los sistemas de cómputo, entre los cuales se usa mucho los sistemas de detección de intrusos.

---

[1] Refiérase a una computadora o a un conjunto de estas orientadas a realizar alguna tarea especifica o algún conjunto de tareas para una organización o alguna persona.

[2] Que algún usuario en Internet, con malas intenciones, entra a nuestro sistema de cómputo a realizar actividades orientadas a dañar, o en muchas ocasiones robar, la información que se encuentra almacenada en el sistema introducido.

[3] Importante rubro dentro del mundo de la computación, ya que se dedica a dar seguridad, mediante una gran variedad de métodos, a la información que se encuentra en alguna computadora.

[4] En el momento en que se lleva a cabo.

[5] Se refiere a algún usuario de Internet, sea dentro de la red o fuera de la misma, que quiere entrar a nuestra red, en caso de que sea un usuario fuera de esta, o ya esté dentro, en caso de que sea un usuario de la propia red, que quiera realizar operaciones, previamente definidas por el administrador de la red, que puedan dañar a nuestra red de computadoras.

[6] Para mayor información dirigirse a la referencia 12.

[7] Es decir, en las computadoras. Esto porque es más fácil de manipular y de ordenar, y para fines prácticos, en una empresa esto es muy útil. Esta manera de manejar la información se lleva a cabo desde que las computadoras empezaron a tener auge.

[8] Propiamente dicho, la información que se manipula.

[9] Generalmente llamados 'hacker'.

La detección de intrusos está catalogada como el área aplicada de la seguridad informática, encargada de informar eventos que pueden tener lugar en un sistema informático y puede ser considerado como parte de un intento de intrusión[10].

Debido a este problema, que ha ido creciendo de manera paralela al crecimiento de Internet, se ha venido desarrollando software[11] para tratar de evitarlo. Y, entre todos los tipos de software desarrollados hasta la actualidad se encuentran los llamados "Sistemas de Detección de Intrusos".

Antes de continuar, es importante aclarar algunos conceptos que nos ayudarán a entender un poco más de lo que estamos hablando[12]:

- **Intrusión.**
Todas aquellas actividades inadecuadas, incorrectas o anómalas que se puedan detectar en nuestro sistema. Generalmente, dichas actividades están orientadas a perjudicar alguna parte de nuestro sistema o, en su defecto, la información que en nuestro sistema se encuentra alojada.

- **Tipos de intrusiones.**
Intrusiones de uso erróneo. Ataques bien definidos contra puntos débiles sabidos de un sistema. Dichos puntos débiles pueden ser efectuados por algún software[13] instalado o por el mismo sistema operativo[14] del sistema.
Intrusiones de anomalía. Desviaciones de los patrones normales de uso de un sistema.
Intrusión física. Cuando el usuario tiene acceso al teclado, es decir, se encuentra frente a la computadora.
Intrusión del sistema. El usuario no tiene privilegios[15] en el sistema pero puede llevar a cabo movimientos que le permitan tener mayores privilegios en dicho sistema.
Intrusión alejada. Penetración de un sistema de manera remota[16].

---

[10] Ingreso a una computadora sin tener los privilegios para hacerlo o siendo una persona totalmente ajena a esta última.

[11] Software que varia mucho dependiendo de las necesidades que se tengan en el momento. Pueden ser desde métodos de autentificación de usuarios, hasta 'firewalls' o 'antivirus'. Cada uno con diferente funcionalidad.

[12] Para mayor información dirigirse a referencia 13.

[13] Generalmente se generan dichas debilidades por software instalado, y esto se debe a que dicho software deja puertos de comunicación abiertos o deja algunos archivos o programas de ejecución que pueden causar vulnerabilidad al sistema de cómputo. Esto sucede muy a menudo cuando los programadores de dicho software no tienen cuidado en el momento en que desarrollan dicho software.

[14] Cuando el punto débil proviene del sistema operativo es más grave el problema. Esto es porque son errores que tiene el sistema operativo; errores que pueden desencadenar otro tipo de fallas dentro del sistema operativo. En estos casos lo más recomendable es los llamados 'parches' de seguridad, los cuáles arreglan dichos puntos débiles.

[15] Permisos que definen las actividades y los derechos que tiene un usuario dentro de un sistema de cómputo. En este contexto, el de la computación, se usa mucho para restringir a cada uno de los usuarios de un sistema en sus actividades dentro del mismo. En ocasiones, los usuarios pueden llegar a cambiarlos realizando algunos movimientos dentro del sistema; lo cuál le permitiría realizar actividades más completas dentro del mismo. Dichas actividades, dada la manera en que se logra la intrusión y las intenciones del usuario que la realiza, pueden ser orientadas a dañar el sistema de cómputo.

[16] Desde otra computadora en la red interna, o bien que se conecte a nuestra computadora por medio de Internet.

- **Tipos de intrusos**

Externos. Tipo de usuario que no tiene autorización a usar ningún recurso[17] del sistema.

Interno. Usuario con autorización para usar solamente algunos recursos del sistema. Se dividen en enmascarados, aquellos que imitan o se hacen pasar por otros usuarios, y clandestinos, aquellos que evaden todo tipo de control.

"Misfeasor". Son los usuarios que emplean mal los privilegios que tienen y con esto pueden provocar vulnerabilidades en el sistema. Es decir, realizan, sin intenciones malas, y en ocasiones sin darse cuenta de que las hicieron, actividades perjudiciales para el sistema.

- **Tipos de detecciones.**

Falsos negativos[18]. En estos casos se logra la intrusión pero, como dicha intrusión no es anómala[19], el sistema no lo detecta.

Falsos positivos. Sucede cuando no es una intrusión pero, dado que es de manera anómala, el sistema decide tomarla como si fuera una intrusión.

Negativos verdaderos. Cuando el sistema indica erróneamente[20] la existencia de una intrusión.

Positivos verdaderos. Cuando existe una intrusión y el sistema, de manera correcta, la detecta.

Una vez definido y entendido lo anterior podemos entrar en materia.

a. Sistema de Detección de Intrusos.

Un sistema de detección de intrusos es aquel sistema o software que nos permite recabar información[21] de distintas fuentes del sistema en el que se implanta para alertar[22] de una posible intrusión en nuestras redes o máquinas. La alerta puede ser del hecho de que existe un intento de intrusión, así como del modo en el que este se está realizando y en algunos casos por parte de quien esta siendo efectuado. Podemos considerar un sistema de detección de intrusos como un 'control de auditoría' que nos permitirá tomar decisiones a la hora de realizar una auditoría de seguridad de nuestro sistema.

Un Sistema de Detección de Intrusos puede distinguir entre un acceso normal y habitual a la red de un intento de vulnerar de algún modo los servicios que ofrece esta misma. Es por esto, que un Sistema de Detección de Intrusos es capaz de alertar al administrador de todos aquellos movimientos, en el tráfico de la red, que sean capaces de vulnerar[23] algún servicio de la red y dejar desprotegida a la misma. Dichas alertas se

[17] Cualquier dispositivo de la computadora en cuestión. Dispositivos que van desde el disco duro o la memoria de la computadora, hasta dispositivos externos como alguna impresora.

[18] Al igual que los 'falsos positivos', 'negativos verdaderos' y 'positivos verdaderos', es nomenclatura utilizada en el contexto computacional.

[19] No esta fuera de las actividades permitidas en la computadora, actividades que en muchas ocasiones las define el sistema operativo, y en muchas otras las define el administrador del equipo o de la red.

[20] El sistema malinterpreta las actividades realizadas en el mismo.

[21] Información acerca de las actividades del sistema.

[22] Enviar alguna señal, ya sea al sistema mismo o al administrador, que haga ver dicha actividad anómala.

[23] Provocar su mal funcionamiento o convertirlo en una puerta de entrada para los usuarios no deseados.

producen en tiempo real; es decir, en el momento en que el paquete llega a la red, el Sistema de Detección de Intrusos lo detecta y genera la alerta.

Es otra herramienta de seguridad, que usan los administradores de red, encargada de monitorear los eventos que ocurren en un sistema informático con la finalidad de detectar una posible intrusión en tiempo real.

Esta es una de las muchas soluciones que se han buscado para tratar de evitar todos aquellos ataques cibernéticos dedicados a adquirir o destruir información que no les pertenece a las personas autoras de dichos ataques. Y, en gran medida han logrado su cometido, y cada ves son mayores los alcances que tienen estos sistemas.

Ahora bien, existen en el mercado una gran cantidad de Sistemas de Detección de Intrusos, cada uno de ellos con características que los distinguen de los demás, que cubren la mayoría de las necesidades de sus usuarios[24]. Más adelante se detallarán dichas características.

Hoy en día los Sistemas de Detección de Intrusos se han convertido en una gran ayuda para los administradores de redes. Lo anterior debido a que es una herramienta muy poderosa para proteger un sistema o una red de amenazas que aparecen en el momento en que se incrementa la conectividad en red, aparte que permite la prevención de ataques cibernéticos que puedan dañar el sistema o deshabilitar algún servicio que provea el sistema atacado.

La eficiencia[25] de un Sistema de Detección de Intrusos radica en la posición del mismo dentro de la red en que se coloque, y se mide acorde a la cantidad de ataques que pueda prevenir. Lo correcto, si se trata de un Sistema de Detección de Intrusos basado en **red**[26] es que se coloque en la puerta de entrada de la red, antes o después de un posible cortafuegos. Esto se ilustra a continuación.

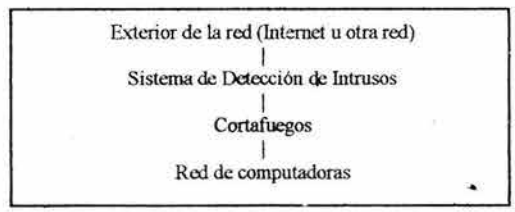

Figura 3-1. Manera correcta de colocar Snort en una red

o bien,

[24] Generalmente administradores de redes.
[25] Manera en que los resultados generados por el Sistema de Detección de Intrusos le sirven a el administrador de la red.
[26] Junto con el Sistema de Detección de Intrusos basado en host son dos de los tipos que existen en la actualidad.

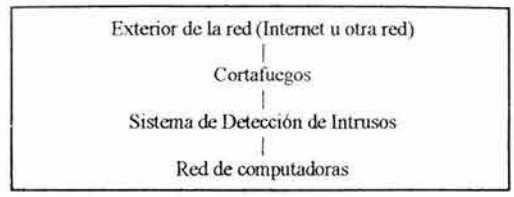

Figura 3-1. Manera correcta número 2 de colocar Snort en una red

Lo anterior es para que el Sistema de Detección de Intrusos cumpla con la tarea de proteger la red con mayor éxito.

En el caso del Sistema de Detección de Intrusos basado en **host[27](computadora)** la colocación del sistema depende de la o las máquinas en donde se quiera tener protegida la información.

Adelante se detallan los conceptos de Sistema de Detección de Intrusos basado en computadora y Sistema de Detección de Intrusos basado en red.

b. Funcionalidad.

Este tipo de sistemas han venido ganando terreno en la aceptación de los administradores de red como una parte importante dentro de la infraestructura[28] de seguridad informática de alguna organización, sea de cualquier tipo.

Un Sistema de Detección de Intrusos tiene varias funcionalidades, entre las cuáles se pueden mencionar las que a continuación se explican de manera breve:

- **Prevenir posibles problemas de intrusiones no deseadas.**
  Debido a que este tipo de sistemas detecta a los paquetes dañinos que desean entrar a la red y los rechaza en intentos posteriores de ingreso a la misma, durante su ejecución los usuarios que intentan este tipo de intrusiones, en su mayoría, no lo vuelven a intentar.

- **Detectar ataques y otras violaciones de seguridad que no son prevenidas por otras medidas de seguridad.**
  Cada atacante intenta sus movimientos mediante técnicas muy conocidas, las cuales este tipo de software las puede controlar, pero a pesar de esto, en muchos casos logran su objetivo porque aprovechan vulnerabilidades[29] no corregidas de algún otro programa, o inclusive del mismo sistema operativo.

[27] Computadora donde se almacena información. En este trabajo se manejará la palabra computadora en lugar de host.
[28] Conjunto de herramientas, tanto de software como de hardware, implementadas en una red para asegurar más la seguridad.
[29] Error que tiene el programa en cuestión que provoca que el sistema operativo quede abierto a cualquier usuario que sepa aprovecharse de dicho error.

Un Sistema de Detección de Intrusos es capaz de detectar alguna intrusión provocada por una vulnerabilidad de algún software instalado en la computadora en donde se provocó la intrusión. Con esto ayuda en mucho a tomar las medidas necesarias, ya sea corrigiendo, "parchando"[30] el programa defectuoso, la vulnerabilidad o desinstalando dicho programa y usando otro que sustituya al anterior en la tarea que estaba realizando dentro del sistema.
Esto también es muy útil para ver que software tiene vulnerabilidades para que los fabricantes de dicho software lo puedan corregir y evitar ese tipo de huecos de seguridad.
Este tipo de sistemas puede detectar, también, ataques que provengan desde un usuario dentro de la misma red, algo que otro tipo de herramientas como los cortafuegos no pueden. Existen varios tipos de ataques que otras herramientas no pueden detectar que este tipo de sistemas si detecta.

- Detectar preámbulos de ataques
Cuando un individuo, ya sea un pirata de Internet, o algún otro tipo de usuarios de Internet, pretende atacar a un sistema lo primero que hace, generalmente, es un 'escaneo' de puertos y servicios que dicho sistema tiene abiertos[31] o provee respectivamente. Entiéndase por 'escaneo de puertos' el proceso de revisión que se le hace a todos los puertos que el sistema tiene abiertos para prestar algún servicio, o bien para adquirir algún servicio.
Dado que dentro de un ataque, esta es la primera etapa que generalmente intenta un atacante, el Sistema de Detección de Intrusos está capacitado para detectar este tipo de movimientos de parte del atacante. Esto quiere decir, que el sistema Snort tiene la capacidad de darse cuenta si el sistema, o la red de computadoras, está sufriendo un 'escaneo de puertos' por algún usuario interno o externo a la red.
Con esto el Sistema de Detección de Intrusos detecta la primera etapa, y a partir de allí empieza a tomar las medidas necesarias para evitar el posible ataque comenzado. Entre otras medidas adoptadas por el software existe el generar una la alerta y dirigirla, ya sea por medio de un envío de correo electrónico o por otro conducto, como una alerta hacia algún dispositivo, al administrador de red, o, de igual manera, el rechazo de los paquetes que provengan del usuario que genera estos movimientos. Este último es el más recomendable, ya que el usuario que realiza dichos movimientos quedará "fichado" como usuario no deseado.
Esta tarea es muy importante porque le hace ver al administrador un posible ataque a la red y, en el mismo momento, puede evitar dicho ataque; con esto el administrador puede tomar otras medidas que considere pertinentes de acuerdo al lugar de donde provenga el ataque, el tipo y la magnitud del mismo.

- Proveer información[32] útil acerca de las intrusiones que se están produciendo.
Cuando existe una intrusión, el Sistema de Detección de Intrusos puede generar reportes y guardarlos en archivos de registro, y, a la vez, generar alertas como

[30] Aplicar el remedio a la vulnerabilidad del programa. Generalmente es otro pequeño programa que se aplica sobre el programa en cuestión y corrige los problemas del programa original.
[31] Que están en servicio. Es decir, que la computadora provee dichos servicios.
[32] Información como la dirección ip de donde se origino el paquete dañino, el movimiento que el paquete quería realizar, la aplicación que deseaba atacar, entre otros.

correo electrónico dirigido al administrador de la red que contengan información de la intrusión. Información que puede estar tan completa o tan básica como se configure en los archivos de configuración del Sistema de Detección de Intrusos. De esta manera cuando el administrador de la red quiera ver un historial de los ataques a la misma, puede consultar los archivos de registro para observar la cantidad de intrusiones llevadas a cabo y el tipo de las mismas.
Así mismo, el administrador puede recibir notificaciones acerca de las intrusiones en tiempo real[33].
La información que el Sistema de Detección de Intrusos le presente al administrador de la red acerca de las intrusiones puede ser tan completa o tan básica de acuerdo al modo en que se configure esa parte en el Sistema de Detección de Intrusos. Generalmente este tipo de sistemas contienen un método de configuración muy completo y detallado para que el administrador de la red, al recibir la información de cada ataque, pueda tomar las medidas de seguridad pertinentes ante cada una de las intrusiones en cuestión.
Esto ayudará a proteger más la computadora de posibles ataques de la misma índole en futuros intentos.

- Generar alertas ante un posible ataque informático.
Como ya se mencionó, los Sistemas de Detección de Intrusos son capaces de generar registros de las intrusiones y guardarlas en archivos para su posterior consulta y, así mismo, generar alertas en tiempo real de diversa índole.
Dichas alertas pueden ser acciones contra el paquete que provoca el ataque informático o contra el usuario que mando dicho paquete, o bien mensajes, mediante correo electrónico o pantallas de mensajes, hacia el administrador de la red para que este pueda tomar las medidas necesarias para evitar dicho ataque. Inclusive, las tres acciones se pueden generar cuando venga un ataque, esto depende de la manera en que el administrador de la red configure su Sistema de Detección de Intrusos.
Esto suele ser de gran utilidad para el administrador de la red debido a que en ocasiones el mismo Sistema de Detección de Intrusos es el que se encarga de evitar los ataques mediante la expulsión automática de los paquetes dañinos. Pero si el Sistema de Detección de Intrusos no es capaz de realizar la expulsión automática de los paquetes, si tendrá la capacidad de alertar al administrador de la red acerca de dichos ataques. Generalmente, cuando se habla de que el Sistema de Detección de Intrusos no es capaz de expulsar un paquete dañino es porque la configuración que el administrador de la red le proveyó al sistema no es completa o no le indica al sistema que expulse dichos paquetes.

- Generar acciones contra algún paquete dañino.
Algunos Sistemas de Detección de Intrusos tienen la capacidad de actuar, en el momento en que detectan la llegada, contra el paquete dañino que entra a la red de varias maneras. Algunas formas de actuar contra el paquete es no dejándolo pasar a la red. Otra es evitando la comunicación entre el usuario que mando el paquete y la red, esto para evitar posibles futuros ataques. Y, así como las ya mencionadas, existen otras acciones que un Sistema de Detección de Intrusos puede realizar en contra de algún paquete dañino para evitar su entrada a la red.

[33] En el momento en que se intente realizar la intrusión, el sistema envía dicha alerta al administrador de la red.

Todo este tipo de acciones varia mucho dependiendo del sof ware que se esté utilizando y de la configuración que se coloca.
Independientemente de que el software utilizado tenga la c: pacidad o no de realizar acciones contra el paquete dañino o contra e usuari que lo envía, la mayoría de este tipo de software tiene la capacidad d alertar de alguna u otra manera al administrador de la red en tiempo real.

- **Detectar y documentar el riesgo que la organización corre.**
Los Sistemas de Detección de Intrusos detectan y registran los ataques cibernéticos hechos a la compañía en donde se instalan, así como las características de dichos ataques. Características co no el usuario de donde provino el ataque, el puerto por el que entró, la aplica ión que intentó explotar, entre otras.
Con todos estos datos, la compañía puede obtener estadísticas acerca de los ataques que le son realizados y, por ende, de las vulne rabilidades que tienen en sus sistemas de cómputo. Y, a partir de estos, utilizarlos para estadísticas o para otras cuestiones.

- **Proteger la red**
En general, es la finalidad de este tipo de sistemas. Y lo logran en gran medida, es por esto que han tenido tanta aceptación entre los administradores de redes.
El nivel de protección que se logra en la red con este tipo de software depende, en gran medida, del producto utilizado, ya que algu os son uy completos y otros solamente tienen las funciones básicas de detecc ón de in rusos. Aún y con esto último todos incrementan, algunos en mayor medida que tros, la seguridad en nuestra red.

La funcionalidades de este tipo de software son muchas, pero la primordial es darle un poco más de seguridad a nuestra red.

c. Tipos de Sistemas de Detección de Intrusos.

Ya que pudimos observar parte de la funcionalidad que tiene este tipo de sistemas, ahora uno se puede preguntar, ¿Qué tipo de sistemas existen?

Los Sistemas de Detección de Intrusos se pueden clasificar de varias maneras. Una primer manera es clasificándolos por aquellos que trabajan en "**tiempo real**" y aquellos que no trabajan en "**tiempo real**".

Los Sistemas de Detección de Intrusos que trabajan en tiempo real, o también llamados activos, son aquellos que tienen la capacidad de estar en constante monitorización del sistema, es decir, están constantemente observando los paquetes que pasan por la tarjeta de red y verificando que dichos paquetes no sean dañinos a la red, y en caso de ser dañinos realizan alguna acción en contra de los mismos o generan algún tipo de alerta como ya vimos anteriormente.

Mientras que los Sistemas de Detección de Intrusos que no trabajan en tiempo real, o también llamados Sistemas de Detección de Intrusos pasivos, son aquellos que únicamente revisan el sistema cuando se les ejecuta, y generalmente esto sucede cuando el administrador de red tiene sospecha de que ha sucedido una intrusión. La desventaja que tiene este con respecto al anterior es que no puede detectar los ataques en tiempo real, solamente los detecta mediante el análisis de las bitácoras cuando ya ha sucedido el ataque, y es por esto que este tipo de sistema no pueden tomar cartas en el asunto de manera directa. Son muy útiles cuando el administrador quiere revisar las bitácoras del sistema, ya que este tipo de sistemas le facilitan en gran medida la tarea.

Existe otra clasificación que comúnmente se les da a los Sistemas de Detección de Intrusos, la cuál está dada de acuerdo al tipo de medios que utilizan los Sistemas de Detección de Intrusos para monitorear los ataques.

Dicha clasificación se podría jerarquizar de la siguiente manera[34]:

- **Sistemas de Detección de Intrusos basados en red.**

Este tipo de Sistemas de Detección de Intrusos usa los paquetes de una red crudos[35] como fuente de datos. Típicamente usan un adaptador[36] de red, es decir la tarjeta de red, en modo promiscuo[37], que constantemente está escuchando y analizando todo el tráfico en tiempo real cuando atraviesa por la tarjeta de red cuando viaja por la red. En este tipo de sistemas un primer nivel de filtro es aplicado para determinar cuales paquetes pasarán a la red y cuales no pasarán dependiendo si contienen patrones de ataques a la misma red de computadoras.

La detección de los ataques en este tipo de sistemas se basa en los patrones de datos que contienen los paquetes destinados a un ataque.

Para que se entienda un poco mejor lo anterior, cada uno de los diferentes ataques informáticos a través de Internet que existen están bien identificados respecto a los patrones que usan para mandar los datos, o respecto de patrones utilizados al hacer las peticiones correspondientes a la computadora que se va a atacar, o respecto a la frecuencia con la que se mandan los paquetes para el ataque, en fin, todo este tipo de cuestiones ya se tienen bien estudiadas, y es de aquí en lo que se basan este tipo de sistemas para detectar los posibles ataques. Siempre basándose en dichos patrones.

La detección de dichos paquetes también depende de la definición de políticas de seguridad[38], en cuestión de filtrado de paquetes, que se hayan definido por el administrador de la red dentro de la configuración del Sistema de Detección de Intrusos utilizado.

Una vez que se han detectado los paquetes dañinos, lo que corresponde al Sistema de Detección de Intrusos es realizar ciertas acciones, definidas también por el administrador de la red en los archivos de configuración, en contra de dichos paquetes dañinos.

---

[34] Para mayor información dirigirse a las referencias 12 y 13.

[35] Sin algún tipo de restricción o manipulación previa.

[36] En los sistemas operativos se le llama "interfaz".

[37] Modo en que una tarjeta de red recibe todos los paquetes que circulan por la red, para que algún programa los tome, los analice, y posterior a esto si los paquetes no pertenecen a la computadora en cuestión los reenvíe a la red.

[38] Conjunto de reglas que definen cuales paquetes son dañinos y cuales no, así como las posibles medidas que se tomas con respecto a dichos paquetes.

- Sistemas de Detección de Intrusos basados en computadora.

Este tipo de Sistemas de Detección de Intrusos en sus principios, en la década de los 80's, generalmente se usaban para revisar los archivos de registro (log) del sistema para detectar posible actividades sospechosas que atentaran contra la seguridad del sistema.

En la actualidad este tipo de sistemas aún usan varios analizadores de archivos de registro pero están mucho más automatizados, son mucho más sofisticados y trabajan en tiempo real en la detección de los posibles ataques y en la respuesta a dichos ataques.

Este tipo de sistemas esta constantemente monitoreando algunos archivos de registro específicos, los cuáles pueden marcar una posible intrusión no deseada.

La manera en que trabajan es mediante el monitoreo constante de los archivos de registro; una vez que detectan que dichos archivos cambian, capturan el cambio y lo comparan con las políticas de seguridad definidas por el administrador de red en los archivos de configuración del sistema, y realizan acciones en consecuencia a ese cambio si tienen que realizarlas. Dichas acciones también están estipuladas en los archivos de configuración del sistema que definen las políticas de seguridad.

Uno de los métodos usados por este tipo de sistemas es que mientras que se monitorea la actividad de registro del sistema otros procesos se encargan de revisar constantemente los archivos de registro para encontrar nueva información y cambios.

- Sistemas de Detección de Intrusos basados en pila.

Este tipo de Sistemas de Detección de Intrusos es de las más novedosas tecnologías de esta área.

Básicamente este tipo de sistemas trabaja por integración cercana a la pila del protocolo TCP/IP, permitiendo a los paquetes ser observados mientras recorren el camino hasta las capas OSI. Esto permite a este tipo de Sistemas de Detección de Intrusos sacar los paquetes de la pila antes de que el sistema operativo o la aplicación a quién van dirigidos los procesen.

Para ser completamente de este tipo de sistema, el software debe de monitorizar tanto la entrada como la salida del tráfico de red en un sistema.

Esto, como puede verse, implica que el software realizará más operaciones, por lo que se necesita una computadora con mayores capacidades para que este tipo de software pueda funcionar de manera regular.

Como ya se explicó, esta clasificación nos agrupa todos los tipos de Sistema de Detección de Intrusos, y como en otras secciones de este documento se menciona, la elección del Sistema de Detección de Intruso que nos conviene usar la haremos de acuerdo a nuestros recursos físicos[39] y económicos y a nuestras necesidades en la red de computadoras.

Es importante hacer una revisión de todos los recursos con que se cuentan y de las necesidades que se tienen antes de realizar la elección del Sistema de Detección de Intrusos, para que ésta sea la mejor para su sistema de cómputo.

[39] Recursos de hardware.

d. Ventajas y desventajas

En el mundo de este tipo de software existen ventajas y desventajas en el uso de los mismos. Y estas ventajas y desventajas se pueden observar desde varios puntos de vista.

Desde el punto de vista económico, es más factible colocar un Sistema de Detección de Intrusos basado en red, esto debido a que si dicho sistema se coloca en un lugar estratégicamente correcto, es decir en la puerta de entrada[40] a la red, sería capaz de darle protección a toda una red de computadoras, ya que si el tráfico de una red de computadoras entra a esta última a través de una computadora, y si en dicha computadora se instala el software, con eso garantizamos la protección a todas las computadoras que se comunican al exterior de la red por medio de la computadora en donde se instala en Sistema de Detección de Intrusos basado en red. Esto nos evita una mayor inversión económica respecto a licencias de software de este tipo para cada computadora. En cambio, si se decide colocar un Sistema de Detección de Intrusos basado en computadora, se tendría que colocar un sistema de este tipo en cada una de las máquinas existentes en la red, y si el sistema elegido es muy caro y la red de computadoras resulta ser grande pues la suma total, en términos económicos, que implicará la instalación de estos sistemas en cada máquina se elevará demasiado. Otro de los factores a tomar en cuenta en este rubro es el tiempo dedicado a la instalación de un Sistema de Detección de Intrusos basado en computadora para cada máquina de la red, ya que si la red es extensa pues implicará mucho tiempo invertido para la instalación correcta y completa de este tipo de sistemas en toda la red. Otro factor importante es el mantenimiento[41] de cada uno de los Sistemas de Detección de Intrusos basados en computadora instalados, ya que, en caso de que sean muchas computadoras en la red, dicho mantenimiento puede llevar mucho tiempo. Estos factores son muy importantes debido a que no todas las compañías tienen el capital suficiente para realizar una instalación tan costosa, y en ocasiones no tienen el tiempo suficiente para llevar a cabo dicha instalación.

Respecto a las ventajas en el campo de la detección de intrusiones, los Sistemas de Detección de Intrusos basados en red pueden detectar intrusiones que los sistemas basados en computadora no podrían ya que los primeros detectan en tiempo real los paquetes que pueden causar problemas en el sistema o en la red, mientras que los segundos se dan cuenta de dichos paquetes al revisar los archivos de registro cuando el ataque ya ha sido ejecutado por algún usuario fuera del sistema. Y un ejemplo muy palpable de esta ventaja es cuando un atacante comienza un ataque del tipo DOS[42] (Denial of Service). El Sistema de Detección de Intrusos basado en red, puede contrarrestar dicho ataque mandando un paquete a la computadora desde donde se originó el paquete para comunicarle una ruptura o cancelación de comunicación[43], y, si está indicado en los archivos de configuración, evitará en un futuro paquetes de la

[40] Computadora que comunica la red con el Internet o con redes externas.
[41] Volver a configurarlo en caso de que algún nuevo tipo de ataque surja en Internet, o bien, en caso de que haya algún otro tipo de acontecimiento.
[42] Ataque que inhabilita algunos servicios de Internet, principalmente el servicio que se provee a través del puerto 80, servicio http.
[43] Cancela la comunicación entre la computadora origen y la computadora donde se encuentra instalado el sistema, y a la cuál quieren provocar el DOS.

misma computadora que originó los paquetes dañinos. Con esto elimina el peligro de que se lleve a cabo por completo la ejecución del ataque. Y aparte queda registrado el intento de ataque. Así, de esta manera, muchos de los ataques conocidos se pueden evitar con facilidad.

Otra ventaja que tienen los Sistemas de Detección de Intrusos basados en red sobre los que son basados en computadora es que a los primeros les es más fácil seguirle el rastro a los autores del ataque. Lo anterior es debido a que como estos últimos sistemas trabajan en tiempo real, las acciones tomadas para el rastreo del responsable del ataque son inmediatas.

En cambio con un Sistema de Detección de Intrusos basado en computadora uno corre el riesgo de no poder rastrear al responsable del ataque si el mismo responsable se encarga de borrar los archivos de registro del sistema así como de borrar las huellas que deja en el sistema, y, dado que este tipo de Sistemas de Detección de Intrusos detecta un ataque mediante la revisión de dichos archivos de registro, pues le sería casi imposible detectar dicho ataque. Esto se da porque en la mayoría de las ocasiones, los intrusos tienen mucho conocimiento acerca del sistema de archivos de registro del sistema operativo que está contenido en la máquina atacada, y es por esto que antes de salir se concentran en borrar cualquier evidencia que les delate su intrusión y estancia en dicho sistema.

Otra desventaja que los Sistemas de Detección de Intrusos basados en computadora presentan es que detectan solamente aquellas intrusiones que tuvieron éxito, es decir, en donde el intruso logra tener acceso por completo a la computadora. Lo anterior es debido a la manera en que funciona este tipo de Sistema de Detección de Intrusos, ya que como se encarga de revisar los archivos de registro después del ataque, hasta ese entonces se puede dar cuenta.

Y, a diferencia de los Sistemas de Detección de Intrusos basados en computadora, los basados en red detectan también los intentos[44] de intrusión a la red. Esto es muy útil debido a que si el Sistema de Detección de Intrusos basados en red se coloca en un punto antes de un cortafuego, es decir se coloca entre el cortafuego y el exterior de la red, este sistema puede detectar un posible ataque y evitar que los datos pasen al cortafuego. Y en caso de que no detecte dicho posible ataque el cortafuego lo puede hacer. En caso de que la configuración de instalación sea contraria, es decir, el cortafuego entre el exterior y el Sistema de Detección de Intrusos, si el cortafuego no detecta el posible ataque, este tipo de sistemas es muy posible que lo detecte. Con esta combinación se incrementa más la seguridad en la red de computadoras en que se instale. Todo lo anterior tomando en cuenta que tanto el Sistema de Detección de Intrusos como el cortafuegos tienen que tener muy bien definidas las reglas que indican las políticas de seguridad de la red de computadoras.

Otra ventaja de los Sistemas de Detección de Intrusos basados en red es que no dependen del sistema operativo de cada una de las computadoras pertenecientes a la red, ya que se instala en una sola máquina y con eso se protege la red. Mientras que los sistemas basados en computadora, tienen esa limitante, ya que ellos si dependen del

[44] Aquellos que no logran su objetivo. Los que fallan en el intento.

sistema operativo que tenga cada una de las máquinas pertenecientes a la red, ya que se instalan en cada una de las mismas.

Por otro lado, los Sistemas de Detección de Intrusos basados en computadoras también tienen ventajas con respecto a los sistemas basados en red. Una de ellas es que los sistemas basados en computadoras avisan de las intrusiones que realmente ocurren, mientras que los sistemas basados en red pueden dar aviso de intrusiones que no lo son, es decir de falsas alarmas.

Otra importante ventaja que tienen los Sistemas de Detección de Intrusos basados en computadora es que pueden monitorear actividades habidas en el sistema con un nivel más específico que las actividades que monitorizan los sistemas basados en red. Esto permite detectar actividades como acceso a archivos, intento de instalación de archivos ejecutables que puedan provocar vulnerabilidades en el sistema o actividades como conocer las tareas de los usuarios conectados a la máquina, e inclusive puede detectar las actividades de entrada y salida de los usuarios existentes en el sistema operativo local. Las anteriores son algunas de las actividades del sistema que un Sistema de Detección de Intrusos basado en red no podría detectar. Esto resulta ser de gran utilidad cuando queremos rastrear las actividades del intruso dentro de nuestro sistema que realizó una vez que logró estar dentro del mismo.

Una de las ventajas más importantes de los Sistemas de Detección de Intrusos basados en computadora es que son capaces de trabajar de manera muy eficaz en las redes de alta velocidad, ya que este tipo de sistemas se encuentra en una computadora de la red y no depende de la topología de la misma, y mucho menos del protocolo que se use en la misma.

Las mencionadas son algunas de las ventajas y desventajas de los Sistemas de Detección de Intrusos basados en red y basados en computadora. A continuación se especifican otras ventajas tanto de unos como de otros.

Otras ventajas de los Sistemas de Detección de Intrusos basados en red[45]:

- Análisis de paquetes.

Los Sistemas de Detección de Intrusos basados en red revisan la cabecera[46] de cada uno de los paquetes del tráfico de la red. Debido a esto es, para este tipo de sistemas, fácil detectar ciertos ataques, los cuáles ya se conocen los patrones que usan en su ataque.

Otra de las ventajas en este rubro, es que también tiene la capacidad de revisar el contenido del paquete, lo que se le llama la carga del paquete[47]. Esto se utiliza mucho para filtrar[48] los paquetes que lleguen a la red o que salgan de ella. Esto evita que los usuarios que se encuentran dentro de la red visiten páginas no

[45] Para mayor información dirigirse a las referencias 12 y 13.

[46] Son los primeros datos que vienen en un paquete de datos que circula por la red de computadoras. Aquí se indican diversas características del paquete de datos como el origen, el destino, el protocolo, entre muchas otras.

[47] Conjunto de datos del paquete que no pertenecen a la cabecera del mismo.

[48] Dejar pasar los paquetes que no se consideren peligrosos y no dejar pasar los paquetes que así se consideren.

permitidas. Otro de los usos es el detectar si los datos mandados por los usuarios cumplen con algunos patrones definidos en las políticas de seguridad.

- **Complementación y Verificación**
Este tipo de sistemas puede ayudar a complementar los componentes usados para la implementación de la seguridad en una red, pues verifica la dirección de origen o el contenido del paquete en caso de que los datos estén encriptados.

Otra de las ventajas que los Sistemas de Detección de Intrusos basados en computadora tienen son las siguientes:

- **Verificación de ataques.**
Antes de que los Sistemas de Detección de Intrusos basados en computadora usen los archivos de registros que contienen eventos que estén ocurriendo, estos tienen la capacidad de conocer si el ataque actual fue exitoso. Esto nos ayuda a evitar la detección de ataques del tipo falso positivo.

- **Ambientes Encriptados.**
En este tipo de ambientes es muy útil un Sistemas de Detección de Intrusos basados en computadora, ya que alguna aplicación puede mandar datos dañinos encriptados a otra computadora, los cuales no sean detectados por un Sistemas de Detección de Intrusos basados en red. Dichos datos llegan a la máquina destino y son desencriptados[49] por la aplicación que los recibe y a partir de ellos realiza una operación y, así mismo, el registro de la operación. Aquí, este tipo de sistemas revisa esos datos después de que se llevó a cabo el desencriptamiento, con lo cual en ese momento puede detectar, una vez desencriptados, si los datos son maliciosos, y si es el caso pues tomar las medidas pertinentes.

- **Monitoreo de Componentes clave.**
Un Sistemas de Detección de Intrusos basados en computadora puede estar constantemente monitoreando los archivos ejecutables, las librerías y los registros de la red del sistema operativo que lo aloja. Esto es muy útil ya que dichos programas son los causantes, en la gran mayoría de los casos, de los ataques fuertes a una computadora, ya que estos son los que ocasionan vulnerabilidades en el sistema operativo. Entonces, al estar en constante revisión de este tipo de archivos, uno puede evitar la existencia de los mismos, también llamados "Troyanos", y con esto evitar las posibles vulnerabilidades que puedan generar en el sistema.

- **Detección y respuesta cercanos al tiempo real**
Dado que estos sistemas están monitoreando de manera constante el registro de archivos, el tiempo de detección se dice que es casi en tiempo real. Esto es debido a que desde el momento en que llega un paquete a la computadora hasta el momento en que se registra un movimiento dentro del sistema relacionado con dicho paquete y la aplicación que lo recibe, pasa un cierto tiempo, generalmente no muy corto, aunque depende mucho de la capacidad de poder de la computadora en cuestión.

[49] Quitarle la condición de cifrado a los datos.

Esto, aunque un poco limitado, en ocasiones es muy útil, ya que el administrador puede realizar acciones en contra del atacante cuando el sistema le envía la notificación de que un posible ataque se está fraguando. Aunque esto último depende de que el administrador se encuentre frente a la computadora en el momento en que es realizado el ataque.

Como ya pudimos ver, tanto los Sistemas de Detección de Intrusos basados en red como los basados en computadora tienen sus ventajas y sus desventajas. Así mismo, cada uno tiene su propia funcionalidad.

Es recomendable, meramente para el incremento de la seguridad en la red de computadoras, y en caso de contar con los recursos necesarios, que se implementen ambos en la red. El Sistema de Detección de Intrusos basados en red en el punto que sale de la red, y los basados en computadora en puntos[50] estratégicos de la red. Esto con la finalidad de que si el Sistema de Detección de Intrusos basado en red no pudo evitar un ataque, el Sistema de Detección de Intrusos basado en computadora nos indique las características del mismo.

e. Software existente

En el mercado existen muchas compañías que han desarrollado este tipo de software, algunas con muchas características útiles, algunas otras con las características básicas que un software de esta índole exige en cuestión a las tareas de la detección de intrusos, algunas otras especializadas para ciertas compañías.

Algunos tienen ventajas sobre otros, pero no dejan de tener las funcionalidades básicas de la detección de intrusos.

Aquí se menciona tres de este tipo de software y se darán algunos detalles acerca de ellos.

- **Snort**
  - Gratuito
  - Lo fabrica Snort.org.
  - Recursos físicos solicitados: muy pocos.
  - Trabaja por medio de la consola
  - Existen interfaces gráficas en web para su manejo.
  - Puede trabajar en conjunto con alguna base de datos.
  - Genera reportes en varios formatos:
    - ASCII
    - XML
    - Base de datos
    - Binarios
  - Muy completo. Provee muchas funcionalidades.
  - Uno puede contribuir con módulos extras.

[50] Computadoras pertenecientes a la red de computadoras.

- Puede desarrollar módulos especializados para su compañía.
- Documentación completa
- Se configura a través de reglas, las cuales definen las políticas de seguridad.
- Código libre
- Basado en red y en computadora.
- Cuenta con lista de Correo.
- El proyecto es mantenido por sus creadores, los cuales son varias personas. El principal es Brian Caswell
- Sistemas operativos que soporta: Linux, OpenBSD, FreeBSD, NetBSD, Solares, SunOS 4.1.X, HP-UX, AIX, IRIX, Tru64, MacOS X Server y Windows

- **ISS RealSecure**
  - No gratuito
  - Lo fabrica ISS
  - Detección exacta de intrusiones.
  - Respuestas sofisticadas a las intrusiones
  - Fácil de mantener
  - Correlación dinámica y análisis
  - Plataformas soportadas: Windows 2000, Linux RedHat 7.3, solaris 7 y 8
  - Espacio en disco requerido: 9 Gb
  - 256 Mb de memoria requerida

- **Cisco NetRanger**
  - Plataforma: Solaris
  - No gratuito
  - Lo fabrica Cisco
  - Mínimo 256 Mb memoria en ram
  - Sistemas operativos soportados: Windows 2000, Windows NT, Solaris

Aquí se han presentado tres marcas diferentes de software de esta índole, pero, al igual que estos tres, existen muchos otros que realizan las operaciones básicas de esta rama de la seguridad informática, e implementan sus propias características.

En el mercado existen muchos más Sistemas de Detección de Intrusos, pero estos son los más conocidos y usados por los administradores de redes.

Hay algunos que necesitan demasiados recursos físicos de la máquina, lo cuál implica invertir también en una buena computadora o en hardware extra para poder soportar de manera eficiente el Sistema de Detección de Intrusos.

A partir de todo esto, un administrador de redes puede elegir alguno.

Capítulo 3

Sistema de Detección de Intrusos SNORT

Objetivo:

Detallar el funcionamiento del Sistema de Detección de Intrusos llamado SNORT, sobre el cual se basa el diseño del sistema planteado en este trabajo.

La capacidad de cada uno de los Sistemas de Detección de Intrusos que existen en el mercado[1] depende en gran medida de la compañía que lo desarrolla.

Snort es uno de los Sistemas de Detección de Intrusos que existe dentro de este mercado, tiene muchas ventajas y también tiene desventajas.

Gratuito, rápido, multiplataforma, funcional, capacidad de generar alertas y acciones en contra de los paquetes dañinos, facilidad de configuración, entre otras son las características que el sistema Snort tiene.

a. Capacidades de Snort

Snort es software libre[2], es decir, no cuesta nada tenerlo y usarlo. Se encuentra en la página www.snort.org, y uno lo puede adquirir en la sección 'Download' de dicha página.

A grandes rasgos, snort tiene muchas capacidades, entre las cuáles se destacan las siguientes:

- Capacidad de análisis de tráfico en una red de computadoras en tiempo real.
- Capacidad de llevar un registro del mismo análisis por direcciones IP[3].
- Puede realizar análisis de protocolos[4].
- Búsqueda de contenidos en los paquetes que analiza.
- Puede ser usado para detectar una variedad de ataques[5] y pruebas[6], ataques que se han vuelto muy comunes en el haber de los piratas informáticos.

Así como las mencionadas, tiene otras muchas capacidades que lo hacen ser uno de los Sistemas de Detección de Intrusos más usado por los administradores de redes de computadoras. Dichas capacidades se detallan un poco más en la siguiente sección.

b. Funcionamiento.

Se basa en filtros que, mediante una serie de reglas, definen las políticas de seguridad puestas por el administrador para la recepción y envío de paquetes de datos. Así mismo, dichas reglas definen la reacción de Snort ante cada uno de los paquetes que concuerde con alguna regla.

El diagrama de funcionamiento del sistema Snort es el siguiente:

---

[1] Internet.
[2] Software gratuito.
[3] Direcciones que en Internet se le asignan a cada máquina conectada directamente al mismo.
[4] Forma en que se comunican, a través de Internet, las computadoras interconectadas.
[5] Ataques de tipo informático dirigidos a la computadora o red de computadoras donde se encuentra Snort instalado.
[6] Pruebas que comúnmente se realizan a la computadora que se desea atacar. Dichas pruebas pueden perseguir varios objetivos, entre los más comunes se encuentra el de ver que puertos están abiertos para ver por donde se puede atacar.

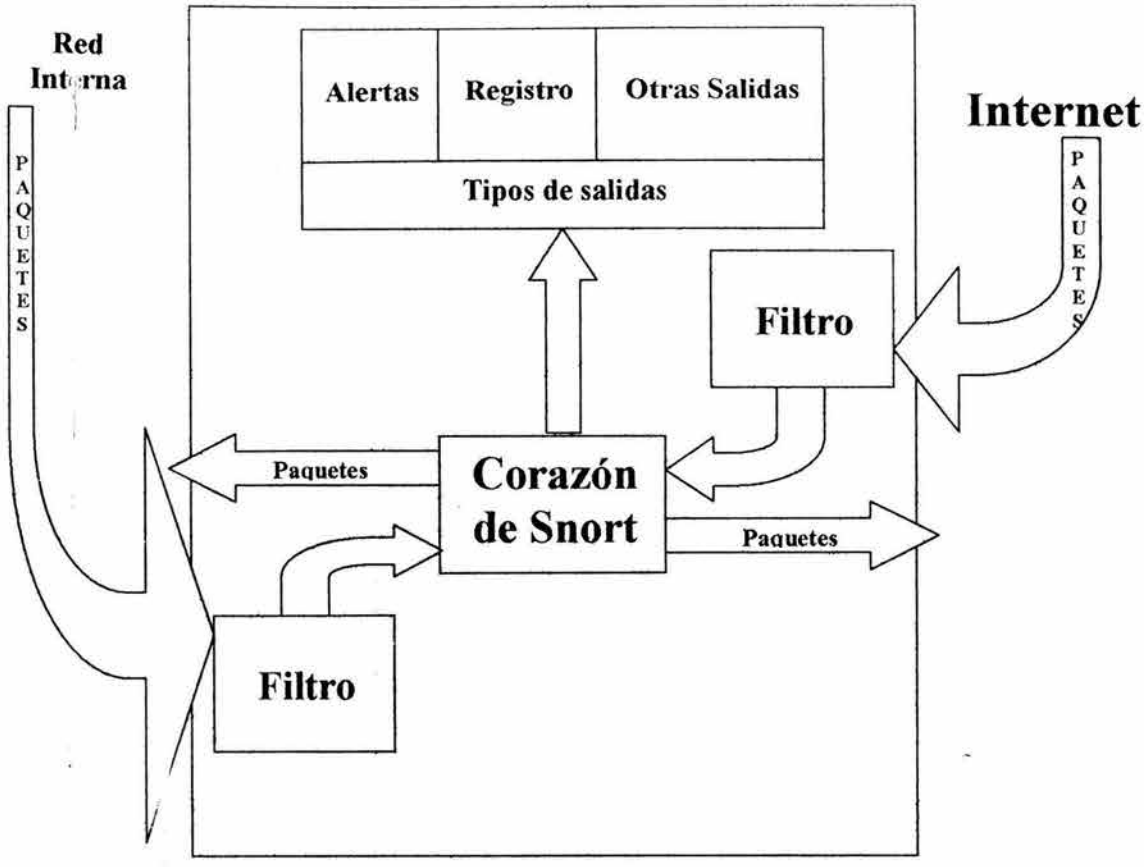

Figura 4-1. Diagrama de funcionamiento del sistema Snort

Este diagrama consta de, básicamente, 3 partes: filtro, tipos de salida y el corazón.

Las reglas se aplican en el filtro, dejando pasar a los paquetes no sospechosos, y deteniendo a los sospechosos.

Los tipos de salida son las formas en que Snort notifica al administrador de que hubo un movimiento extraño o perjudicial para la red de acuerdo a las reglas previamente estipuladas. Existen varios tipos de salida ya establecidos, como por ejemplo alertas en ventanas del sistema operativo, mail, base de datos, registro en archivos, entre otras.

Y por último el corazón de Snort, el cual se encarga de verificar que tipo de salida merece el paquete que, según el filtro, puede ser perjudicial para la red. Se encarga, así mismo, de llevar a cabo la ejecución de dicha salida.

Cuando un paquete entra a la red desde Internet, pasa por el filtro, y este es el que se encarga de verificar si el paquete es inofensivo o no. Una ves determinado esto, en caso de que resulte ofensivo a la red, le notifica el paquete al corazón de Snort y este, de acuerdo a las acciones estipuladas en las reglas de configuración, ejecuta la acción correspondiente. En caso de que el paquete no sea determinado como perjudicial para la

red, el filtro lo deja pasar a la red. El proceso inverso, es decir cuando los paquetes provienen de la red y se dirigen a Internet, es igual. Antes de pasar del otro lado tiene que ser revisado por Snort.

Son muchas las capacidades que tiene Snort, así como las funcionalidades con que cuenta, es por esto que esta sección se ha optado por dividirla en varias partes.

Funcionalidad.

Snort funciona por medio de la consola[7] del sistema operativo, es decir que el usuario le envía las instrucciones a través de la línea de comandos. Por medio de estas últimas, el usuario le indica a Snort la manera en que trabajará, es decir, cual va a ser su comportamiento, de donde va a obtener los archivos de configuración, donde va a colocar los registros que el genere, entre otras funciones.

La configuración[8] de Snort queda estipulada dentro de los archivos de configuración, que generalmente se encuentran en el directorio llamado 'conf' dentro del directorio de instalación, y están conformados por archivos de reglas, archivos de configuración de módulos, y por el archivo principal, el cual manda llamar a todos los demás archivos de configuración.

El comando con el que se llama a Snort es el que lleva su mismo nombre, 'snort'. Uno, al querer iniciar el funcionamiento de Snort mediante la consola uno puede teclear lo siguiente:

directorio_de_instalación/bin/*snort banderas_de_funcionamiento*

donde 'banderas_de_funcionamiento' son las posibles banderas para activar o desactivar las diferentes funcionalidades de Snort, así como para indicarle la manera en que debe de comportarse.

Cada una de las banderas de funcionamiento indica a Snort acerca de archivos de configuración, modalidades de funcionamiento, acciones a tomar, archivos de salida, entre otras cosas.

Una vez que Snort es llamado, la manera en que trabaja es la siguiente:

- Coloca la tarjeta de red en modo promiscuo[9].
- Toma cada uno de los paquetes que pasan por la tarjeta y los analiza.
- Si alguno de los paquetes analizados coincide con alguna, o varias, de las reglas definidas en los archivos de configuración es lanzada[10], o lanzadas.
- Una vez lanzada dicha regla, Snort realiza las acciones que la regla en cuestión le indique, acciones que son definidas por el administrador del sistema.

[7] Es la interfaz gráfica o de texto que es útil para que haya comunicación entre el usuario y el sistema operativo a través de comandos.
[8] Manera en que trabajará el Snort.
[9] Quiere decir que puede leer todos y cada uno de los paquetes que pasen por dicha tarjeta de red, aunque no vayan dirigidos a la computadora en donde se encuentra.
[10] Es activada, para su uso.

- Una vez realizadas todas las acciones indicadas por la regla lanzada, Snort queda en un estado de espera, en donde recibirá el siguiente paquete de la red a analizar.

El ciclo anterior se repite hasta que Snort es detenido por el sistema operativo o por el administrador del sistema Snort. De esta manera, Snort podrá analizar todos y cada uno de los paquetes de datos que circulen por la red de computadoras.

Snort, en su gran variedad de funcionalidades, puede trabajar en tres modos distintos, con diferentes capacidades cada uno. Cada uno de los modos de funcionamiento se explica en la siguiente sección.

La manera de configurar a Snort es a través de reglas, en las cuales, el administrador del sistema Snort, que en la mayoría de las ocasiones es el mismo que administra la red, le indica la manera en que trabajará respecto a los paquetes que circulen por la red. Esto es, cuáles paquetes los va a tomar como dañinos a la red y cuáles no, de que manera va a reaccionar con cada uno de los paquetes y las posibles acciones tomadas. Las partes que el sistema puede revisar de cada paquete son muchas, y van desde la revisión de su contenido hasta la revisión del protocolo. Más adelante, en la sección 'Métodos de configuración' se detallarán un poco más estas cuestiones.

Modos de uso.

Snort tiene la capacidad de trabajar de tres maneras, modo 'sniffer[11]', en modo de registro de paquetes[12], y en modo de detección de intrusos[13]. Cada uno de los modos de trabajar de Snort tiene sus propias ventajas y desventajas.

Así mismo, cada uno de estas maneras de trabajar del sistema Snort tiene, para el uso de la consola, sus propias banderas de funcionamiento.

1.Modo Sniffer.

En este modo de funcionamiento, el sistema Snort simplemente lee los paquetes de datos que pasan por la red de computadoras y los despliega[14] a través de un 'stream[15]' continuo a través de la consola.

Dentro de las opciones que este modo de funcionamiento tiene, y las cuales cada uno tiene su propia bandera de funcionamiento, existe las siguientes:

V Indica a Snort que deberá imprimir la cabecera[16] de cada uno de los paquetes que analiza dentro del tráfico de la red. La peculiaridad de esta bandera es que le dirá a Snort que imprima solamente la dirección IP y las cabeceras TCP/UDP/ICMP[17].

[11] Modo en el cuál está viendo todos los paquetes.
[12] También llamado 'Packet logger' (En idioma inglés).
[13] También llamado Network Intrusión Detection (en idioma inglés).
[14] Es decir, envía lo que en el momento lee. Generalmente lo envía con cierto formato.
[15] En español, flujo. Es un conducto por el cuál cualquier programa en un sistema operativo puede enviar o recibir datos.
[16] Es la primera parte que los paquetes de datos tienen. Es donde viene información del paquete, información como la dirección ip de origen, la dirección destino, el protocolo, entre otros.
[17] Distintos tipos de protocolos con los que se puede transmitir datos a través de Internet.

D Indicará a Snort que despliegue, o que mande por el 'stream' correspondiente, los datos del paquete así como las cabeceras.
E Indica a Snort que despliegue los datos de la operación en transacción, es decir la operación a la que va dirigida el paquete analizado.

Estas tres banderas de funcionamiento se pueden combinar[18] para aumentar la funcionalidad de este modo de uso de Snort. Así, con una combinación de las tres, Snort imprimirá la cabecera, los datos del paquete y los datos de la operación en transacción del paquete que se está analizando en el momento.

En este modo de funcionamiento, Snort, generalmente, despliega todos los datos en la consola a la velocidad en que los va procesando, lo cuál puede resultar no legible para el administrador de la red.

2.Modo de Registro de Paquetes.
En este modo de funcionamiento, Snort guarda los paquetes en el disco duro de la computadora en donde se encuentra instalado.

Esta funcionalidad es muy útil cuando uno quiere analizar los resultados arrojados por el sistema Snort. Esto para ver con mayor calma la manera en que el ataque, en caso de que haya habido alguno, fue perpetuado, o para ver los posibles intentos de intrusión al sistema o a la red.

Las banderas que definen cada una de las capacidades de este modo de funcionamiento de Snort, se detallan a continuación:

l ruta_de_directorio Le indica a Snort en que directorio se guardarán los registros que se puedan generar. La manera en que los almacena es la siguiente: en dicho directorio genera un directorio para cada dirección ip que genere un registro, y en dicho directorio guardará en un archivo los registros que se generen para dicha dirección ip en algún puerto específico. Los directorios generados llevarán por nombre la dirección ip correspondiente al paquete que lo genera.
h dirección_ip_de_la_red Le indica a Snort que red va a monitorear. Con esto Snort solamente registrará los paquetes que provengan de la red indicada, y, en caso de que no provengan de dicha red, los dejará pasar. El formato que se usa para indicar la dirección ip de la red a monitorear es el llamado CIDR[19].
B

[18] Colocar cualquier combinación de ellas en la línea de comandos para que Snort las lea.
[19] Classless Inter.-Domain Routing en ingles. Es un formato eficiente de representar direcciones ip de Internet para redes de clase A, B, C.

Indica a Snort que guarde los paquetes en modo binario, es decir en un formato de 0's y 1's. Esto es muy útil cuando uno quiere ahorrar espacio en disco duro, ya que este formato de registro ocupa menos espacio que el formato de registro en texto.
Cuando uno quiera volver a leer los registros, tendrá que indicarle a Snort esta misma bandera para que este último pueda traducirlo a formato texto y que uno le pueda entender.
Esta bandera permitirá a Snort trabajar de manera más rápida, ya que esta bandera solamente analizará lo mínimo necesario de cada paquete y lo guardará sin cambiarlo a formato texto ASCII.

r paquete.log indicador
Indica a Snort, mediante 'paquete.log', que convierta el archivo de registro en formato binario, guardado previamente con la bandera 'b', en un formato texto ascii. De esta manera Snort trabaja en modo 'sniffer'.
El 'indicador' le dice a Snort que protocolo quiere analizar en el archivo donde se registraron los paquetes. Esto es, sólo leerá los paquetes registrados que concuerden con el protocolo indicado.

3.Modo de Detección de Intrusos.
En este modo de funcionamiento, el cual es el más complejo y configurable que Snort tiene, puede analizar el tráfico de la red de computadoras para actuar contra los usuarios que puedan generar paquetes dañinos, así como le permite realizar ciertas acciones para evitar dichos paquetes.

Las banderas de funcionamiento que responden a este modo de uso de Snort son las siguientes:

c archivo_de_configuración
Indica a Snort el archivo en donde se encuentra la configuración que adoptará para su funcionamiento. Allí se encuentran definidas las reglas que Snort aplicará a cada uno de los paquetes que pasen por la tarjeta de red.

Dentro de este modo de funcionamiento, Snort puede modificar los mecanismos de salida de datos generados.

Para entender de mejor manera lo anterior es necesario saber que Snort, al generar una alerta imprime, según su manera estándar, el mensaje de alerta junto con la cabecera del paquete de manera completa, lo cuál puede hacer que Snort se vuelva lento si la red es muy propensa a ataques, ya que Snort estará generando alertas constantemente.

En cuanto a los métodos de salida que Snort ofrece son seis, y se le indican a través de una bandera de funcionamiento, los cuáles se detallan a continuación.

A fast|full|unsock|none|syslog|smb
Indica a Snort el medio y la manera por el cuál enviará los datos generados en

los registros.
fast. Permite a Snort escribir la alerta en un formato simple con la hora en que sucedió la alerta, el mensaje de alerta, la dirección IP fuente[20] y destino[21] y sus respectivos puertos.
full. Es el modo de alerta predeterminado. Comprende todos los datos que la alerta genera, desde la hora en que se generó, hasta los datos del paquete que la generó. Hace que el funcionamiento de Snort sea menos eficiente.
unsock. Envía la alerta por medio de un socket, el cual se le indica después de la bandera de funcionamiento. Con esta opción, otro programa en alguna otra parte de Internet puede estar atento a recibir dichas alertas para generar alguna acción, o simplemente para saber que se generó una alerta.
none. Indica a Snort que no debe de generar alertas, es decir, apaga el modo de alerta de Snort. Provoca que Snort se haga muy eficiente porque no tiene que generar las alarmas, pero por otro lado, uno se expone a que venga un paquete dañino sin que se genere aviso alguno.
syslog. Envía la alerta al sistema de registro del sistema operativo. Con esto la alarma quedará registrada en el sistema operativo, y no en el sistema de archivos de registro de Snort. Este modo de salida también se le puede indicar mediante la bandera de funcionamiento 's'.
smb. Indica a Snort que debe de enviar las alertas por medio de un puerto samba[22], es decir un puerto que se pueda comunicar con máquinas que tengan el sistema operativo Windows.

En muchas ocasiones uno desea que Snort trabaje lo más óptimo y rápido posible en este modo de funcionamiento. Para esto las opciones antes mencionadas nos ayudan mucho en la solución de esta inquietud.

Por ejemplo, si uno, en la línea de comandos teclea

snort –b –A fast –c snort.conf

le indica a Snort que registre los movimientos con el formato más simple (opción **fast**) y que lo guarde en modo binario (opción ***-b***). Con esto estaríamos haciendo que Snort se agilizara notablemente.

En ocasiones, a los usuarios de Snort no les agrada la manera en que Snort aplica las reglas a los paquetes, ya que Snort aplica, de acuerdo a su configuración predeterminada, las reglas 'alert[23]' en primera instancia a los paquetes, luego las reglas de tipo 'pass[24]', y por último aplica las reglas de tipo 'log[25]'. Bueno, pues para esas personas, Snort nos proporciona otra bandera de funcionamiento.

[20] Máquina de donde provino el paquete.
[21] Máquina a quién está dirigido el paquete.
[22] Protocolo utilizado para comunicar sistemas operativos de tipo UNIX con el sistema operativo Windows.
[23] Las reglas que generan alerta por los paquetes analizados.
[24] Las reglas hacen que Snort ignore los paquetes.
[25] Las reglas que registran el paquete, sus datos y cabecera.

O
Cambia la manera en que Snort aplica las reglas a los paquetes que analiza. La nueva forma en que Snort aplica las reglas, una vez indicada esta bandera de funcionamiento, es el siguiente: primero aplica las reglas de tipo 'pass', luego las reglas de tipo 'alert' y posteriormente las reglas de tipo 'log'.

Cada una de las banderas de funcionamiento de estos tres modos de uso de Snort se pueden combinar en la línea de comandos para aumentar la funcionalidad de el mismo. En este rubro, aunque uno tiene la libertad de combinarlas, tiene que tener en cuanta que ciertas combinaciones no son muy convenientes porque hacen menos optimizado el funcionamiento de Snort o pueden realizar cosas que uno como administrador del sistema Snort no desea que pasen.

Extras de las instrucciones de consola.

Snort provee de un par de banderas de funcionamiento extras que aumentan un poco más la funcionalidad del mismo.

Son muy útiles para el administrador del sistema Snort, ya que una de éstas permite correr[26] Snort en modo demonio[27] (bandera de funcionamiento **D**), y la otra bandera publica los registros de los paquetes en una lista de correo pública (bandera de funcionamiento **O**).

Con la bandera de funcionamiento **'D'** uno debe tener cuidado, ya que la manera correcta de echar a andar Snort con esta bandera de funcionamiento es mediante rutas absolutas, es decir de la siguiente manera:

ruta_absoluta_de_direcotiro_de_instalación_snort/bin/snort banderas_de_funcionamiento -D

Esto es porque el sistema operativo, por seguridad en el mismo, no acepta rutas relativas cuando se va a echar a andar un programa en modo demonio.

La bandera de funcionamiento 'O' indicará a Snort que debe de ocultar nuestra dirección IP en las impresiones de salida del paquete, esto es, no imprimirá nuestra dirección IP cuando registre un movimiento. Esto resulta muy útil porque, en el momento en que publica los resultados en una lista de correo pública, uno no se tiene que preocupar por que los usuarios de dicha lista puedan ver la dirección IP de nuestra red.

Una última bandera de funcionamiento que nos ofrece Snort es la bandera '?', la cuál nos despliega una ayuda en la consola, esto para ver todas las banderas de funcionamiento que acepta Snort, así como una pequeña explicación de cada una de ellas.

[26] Ejecutar un programa, en este caso Snort.

[27] También se le llama en modo 'background'. Esto quiere decir que se ejecuta en memoria y deja libre la consola para ejecutar otros procesos.

Métodos de configuración.

Snort se puede configurar de una manera muy sencilla. Esto ayuda a que su configuración sea lo mas acorde a las necesidades de la red de computadoras en cuestión a su seguridad contra ataques.

La configuración que utiliza Snort es mediante archivos ligados[28] entre si, los cuales le indican lo que tiene que hacer y lo que no tiene que hacer, cuales paquetes son malos y cuáles son buenos. En fin, le indican a Snort la manera de trabajar.

Snort se configura a través de un solo archivo, indicado en la línea de comandos mediante la bandera de funcionamiento 'c', que comúnmente se encuentra en el directorio 'conf' dentro del directorio de instalación de Snort. Este archivo puede estar estructurado de dos maneras: la primera es teniendo en él mismo todas las reglas e instrucciones necesarias que Snort tenga que leer para que empiece su buen funcionamiento; y la segunda es una serie de llamadas a otros archivos donde se tengan las reglas y las otras instrucciones necesarias para el Snort. La primera no es muy usada porque, en la mayoría de las ocasiones no es muy legible[29] el contenido de dicho archivo, por lo que cuando uno quiere cambiar algo suele batallar. La segunda manera es muy usada ya que permite tener de manera más ordenada todas las instrucciones que se le pasaran a Snort para su configuración. De esta forma, mediante unas instrucciones que Snort entiende, se llama el contenido de otros archivos, y, de esta manera, Snort interpreta dichos contenidos como si estuvieran en el archivo principal. Esta segunda forma nos permite tener modularizado[30], por decirlo de alguna manera, todo el contenido de la configuración de Snort. Esto es, tener las reglas de cada tipo en un solo archivo para que cuando uno quiera cambiar alguna regla que veamos que esté fallando, uno se pueda dirigir al archivo que contiene las reglas de su tipo, se busque la regla deseada y se cambie.

Snort es capaz de detectar, usando la primera o la segunda opción, si alguna instrucción o regla de configuración se encuentra mal escrita. Cuando así las detecta, interrumpe su funcionamiento y despliega el error en la consola. Esto para que se pueda corregir y volver a arrancar Snort.

La descripción del archivo principal se encuentra con mayor detalle en los apéndices B (Archivo principal de configuración del sistema Snort) y C (Componentes de las reglas de configuración de Snort) en la parte final de este trabajo.

En estos apéndices uno podrá observar la manera en que las reglas son creadas, así como todas sus partes y opciones posibles, dentro de la configuración del Sistema de Detección de Intrusos Snort.

En cuanto a las capacidades que Snort tiene se puede mencionar lo siguiente.

[28] Quiere decir que unos mandan llamar el contenido de otros.

[29] No es muy entendible su contenido, así como la estructura que tiene el mismo.

[30] Separar las cosas en módulos. En este caso, tener cada tipo de regla en un solo archivo. Así se tienen todas las características de configuración en muchos archivos, de manera más legible y manejable para el administrador de Snort.

Capacidades.

Snort es uno de los Sistemas de Detección de Intrusos más usados en el mundo de la seguridad informática para proteger a las redes de computadoras. Este puesto se lo ha ganado gracias a todas las capacidades con que cuenta.

Capacidades que van desde su eficiencia y rapidez hasta su fácil configuración. A continuación se listan algunas de dichas características.

Eficiencia y seguridad.

Snort es un software que resulta ser muy eficiente ya que, si se configura bien, logra detectar todos los posibles ataques informáticos que se le indiquen.

Otra de las características que detallan a Snort es que es muy seguro, tanto en su funcionamiento como en la detección de ataques informáticos.

Este par de características lo hacen muy atractivo a su uso.

Rapidez.

Snort resulta ser muy rápido debido a que esta hecho con el lenguaje C, esto hace que su funcionamiento sea de manera veloz.

Fácil de arrancar.

Snort, en su arranque puede recibir banderas de funcionamiento. Su arranque se realiza a través de la consola del sistema operativo. Las banderas de funcionamiento nos permiten darle mayor funcionalidad.

Tres modos de funcionamiento

'Sniffer', 'Registro de paquetes' y 'Sistema de Detección de Intrusos' son los tres modos en que Snort puede funcionar. Cada uno posee sus características.

El modo de Sistema de Detección de Intrusos es el más complejo y el más configurable. Este nos permite asegurar la red de computadoras sobre la que se instala Snort. Este modo de funcionamiento es el que más se usa de los tres.

El modo de 'Registro de paquetes' es sencillo y solamente registra los paquetes de datos que circulan por la red de computadoras en el disco duro, ya sea en varios archivos o en uno solo.

El modo de 'Sniffer' es el más sencillo de los tres. En este modo solamente recibe los paquetes y los despliega en la consola para que el usuario los pueda visualizar.

Modularización de archivos de configuración

Snort permite repartir en varios archivos todas las instrucciones y reglas que se le dan a Snort para su buen funcionamiento. De esta manera uno puede tener más organizado todas las partes de la configuración de Snort.

Fácil creación de reglas

Snort funciona a través de reglas, las cuales le indicarán cuáles paquetes resultan ser dañinos y cuáles no.

Estas reglas son muy sencillas de crear, tienen una gran gama de opciones y permiten crear una gran variedad de defensas contra los posibles ataques informáticos.

Se pueden crear cuantas reglas sean necesarias.

Constan de dos partes, la cabecera y las opciones, y tanto una como la otra son sencillas de construir, y tienen una gran funcionalidad integrada.

Detección de muchos tipos de ataques

Snort permite detectar muchos tipos de ataques informáticos por medio de sus reglas de configuración. Ya que estas últimas son las encargadas de indicarle a Snort los patrones que usan los paquetes de datos que producen cualquier ataque informático.

Alertas en tiempo real

Capaz de alertar al usuario en el momento en que detecta que uno de los paquetes cumplió con lo que alguna regla indica. Snort genera una alarma y se la envía, de diversas maneras, al administrador del sistema Snort.

c. Ventajas y desventajas de Snort.

Ya vimos que Snort tiene muchas ventajas, pero también tiene desventajas.

Algunas de las ventajas que pudimos observar que Snort contiene son las mencionadas en la sección anterior llamada 'capacidades'. Existen otras ventajas que Snort tiene como las siguientes:

No tiene costo

Snort es un software que no tiene costo alguno, por lo que es muy fácil de adquirir.

Para adquirirlo solo se tiene que entrar a su página en Internet e ir a la sección llamada 'download' y adquirir el software.

Uno lo puede adquirir e instalar casi sin ningún problema.

Soporte en línea

Cuentan con una lista de correo electrónico en donde uno puede preguntar cualquier duda que le surja acerca del comportamiento de Snort.

En caso de que Snort genere una falla o un error, o algún problema de seguridad para el equipo donde se instaló, uno lo puede comunicar a la lista de correo, y los mismos creadores de este software se encargan de corregir dicho detalle.

Actualizaciones del Software constantemente

Los creadores de Snort, junto con el equipo de trabajo que ayuda a su desarrollo, están en constante avance en las nuevas versiones de Snort. De manera seguida actualizan Snort, ya sea que le agregan módulos, le arreglan fallas que se reportaron.

Interacción con base de datos.

Snort puede registrar los movimientos en base de datos en lugar de archivos.

Y, aunque todavía son pocos los manejadores de base de datos con los que puede interactuar, estos últimos son los más usados en el mercado de las bases de datos.

El principal manejador de base de datos con el que Snort puede interactuar es el muy conocido MySQL[31], el cuál también es gratuito y se adquiere en www.mysql.com.

Portabilidad

Snort tiene versiones para casi todos los sistemas operativos que existen. En el capítulo 3 se presentaron los sistemas operativos para los que Snort tiene alguna versión. Cada versión, en este caso, significa que toda la funcionalidad la adaptaron al sistema operativo particular.

[31] Es uno de los manejadores de base de datos más usados en Internet. Gratuito y con versiones para una gran variedad de sistemas operativos. Quizá por eso Snort sea con el que más interactúa.

Fácil de aprender a usar

Snort es tan sencillo de usar que toda aquella persona que realmente desee aprender a usarlo no batallará mucho.

Esto permite que los administradores de redes adquieran de manera rápida los conocimientos necesarios para manejar este tipo de software.

Reglas predeterminadas

En el sitio de Internet www.snort.org, lugar donde se encuentra la página de Snort el equipo de desarrollo proporciona una gran variedad de reglas predefinidas por ellos, las cuáles se pueden usar cuando el software se encuentra instalado.

Dichas reglas tienen la característica de cubrir, referente a la seguridad, ciertos movimientos en la red que puedan resultar ser dañinos para la misma. Estas reglas ya son seguras a la hora de realizar su trabajo, ya fueron probadas y están a disposición del que las quiera usar.

Y, ya que no todo en la vida es de color rosa, Snort también tiene, aunque muy pocas, desventajas.

Una de sus principales desventajas con respecto a otros sistemas de este tipo es que salvo las alertas en tiempo real que puede generar y mandar a un mail o a otro tipo de salidas, Snort registra todos sus movimientos en disco duro. Esto es, cuando Snort detecta un paquete dañino, generalmente guarda los datos necesarios que el usuario le pidió que guardara. Cuando dicho usuario quiera ver que movimientos hubo tiene que consultar las bitácoras, y esto puede ser algo inconveniente cuando la necesidad exige actuar de inmediato.

Otra de las desventajas que Snort tiene es que no cuenta con una interfaz gráfica de usuario (GUI[32]) que le permita a éste último interactuar con el software de manera visual. Existen varias aplicaciones que han hecho varias compañías, pero siguen estando algo incompletas, es decir, tienen desventajas como que no trabajan en tiempo real porque se basan en web, no permiten realizar todas las operaciones que Snort te permite, entre otras desventajas que presentan.

Snort es un software muy completo, realiza las funciones de un buen Sistema de Detección de Intrusos, es eficiente, rápido, confiable, y puede usarse en varios sistemas operativos. Por estas y muchas otras características ha logrado la aceptación de muchos usuarios.

[32] Graphic User Interface por sus siglas en inglés.

Capítulo 4

Sistema GSNORT

Objetivo:

Presentar el diseño, la manera en que trabaja, las ventajas, las desventajas y otras características que tiene el sistema, llamado GSNORT , planteado en este trabajo.

Realizando una breve y concisa recapitulación, en los capítulos anteriores hemos visto algunos de los detalles que se deben tomar en cuenta cuando se habla de seguridad informática aplicada a redes de computadoras. Así mismo, le dimos un vistazo a los sistemas operativos que trabajan en red y a las herramientas que nos pueden ayudar a llevar a cabo una implementación de la seguridad en la red de computadoras.

Vimos que los Sistemas Detectores de Intrusos de Red (NIDS[1]) son herramientas muy útiles para incrementar un poco más la seguridad en una red de computadoras, le dimos un vistazo a las características que deben tener dichos sistemas, y, de igual manera, observamos que las características de cada software Detector de Intrusos depende de la compañía que lo desarrolle.

Así mismo, recorrimos muchas de las bondades que el Sistema de Detección de Intrusos llamado Snort nos proporciona. Bondades como la confiabilidad de este software, así como su seguridad y eficiencia a la hora de trabajar.

Snort es un sistema muy completo, cuenta con las características básicas que un Sistema de Detección de Intrusos debe tener.

Una de las desventajas que Snort presenta es que no tiene una interfaz gráfica de usuario[2] para la administración del mismo, solamente cuenta con la interfaz de consola[3], en donde uno puede ejecutar Snort brindándole opciones[4], a través de banderas de funcionamiento, para que su funcionalidad sea más acorde a lo que nosotros como usuarios del sistema Snort queremos. Esto en gran medida, nos permite manipular, referente a la manera en que va a actuar, a Snort de una manera más completa, aunque no dejará de resultar un poco incómodo para todas aquellas personas que no estén acostumbradas a trabajar en una consola, a través de la línea de comandos, del sistema operativo en el que se está trabajando.

Se han realizado diversas interfaces de usuario que trabajen con el sistema Snort, pero la mayoría trabaja mediante el web, es decir, son aplicaciones hechas para Internet, para tener acceso a ellas por medio de un navegador[5]. Son amigables cada uno de las aplicaciones que se han desarrollado, algunas más que otras, pero tienen la desventaja de no poder trabajar en tiempo real[6], ya que el protocolo http[7] no se los permite.

Y, como ya se explicaba en el capítulo anterior, la desventaja mencionada en el párrafo anterior resulta ser, en muchas ocasiones, una desventaja seria, ya que si uno como administrador de Snort quiere ver lo que está arrojando[8] en el momento en el que lo hace pues resulta imposible a través del web, ya que este protocolo no permite la actualización.

---

[1] Network Intrusion Detection System por sus siglas en inglés.
[2] Programa gráfico y amigable que ayude a la interacción entre el usuario y el sistema en cuestión.
[3] Interfaz de linea de comandos.
[4] Opciones por medio de banderas de funcionamiento, las cuáles cada una le indica a Snort algún detalle de su mismo funcionamiento.
[5] Programa utilizado para acceder a páginas de Internet. Los más usados son tres: Internet Explorer (Microsoft Company), Netscape Navigator (Netscape) y Mozilla.
[6] Desplegar los resultados en el momento en que Snort los arroje.
[7] Protocolo utilizado para transportar datos a través de Internet.
[8] Los resultados que Snort genera.

Continuando con este punto, esta desventaja se ve reflejada en las alertas que genera Snort, ya que cuando genera una alerta tiene varias maneras de darla a conocer: registrarla en archivos o en alguna base de datos, enviar un mail al administrador con las características de la alerta, o un mensaje a través de una ventana que se despliegue en la pantalla; sin embargo, no le notifica al administrador de manera directa. Cualquiera de las tres presenta detalles que retrasan una posible intervención del administrador en el problema que genera la alerta. En el primero, el administrador se da cuenta de que existió una alerta hasta el momento en que revisa los registros, ya sea en la base de datos o en los archivos correspondientes y, en caso que hubiera sido necesaria su propia intervención en el momento preciso de la generación de la alerta, esta última no se pudo haber llevado a cabo. En la segunda, el administrador se da cuenta, suponiendo que tenga algún sistema que se lo permita, que le llego un mail con la alerta, lo revisa y observa el tipo de alerta del que se trate; aquí, el revisar el mail lleva tiempo, y si la alerta generada requiere una intervención inmediata, pues no es posible una intervención apresurada dado el tiempo que se lleva en la revisión del mail. En la tercera, los mensajes que se despliegan en la pantalla son solo ventanas de mensajes, y no te permiten realizar nada al sistema Snort o, en ocasiones, a la computadora de donde viene el ataque, por lo que, aunque son muy útiles para dar aviso no dejan de ser incompletos.

Es por esto que es conveniente que exista una interfaz gráfica de usuario que permita al administrador del sistema Snort tener el control de el y le permita, de manera visualmente atractiva[9], realizar acciones en caso de alertas, en caso de corrección de la configuración, en caso de manipulación de archivos, y en otros aspectos.

A este punto, este trabajo propone el diseño de un sistema que elimine la mayoría de dichas desventajas y que le proporcione al administrador del sistema Snort una manera de interactuar con el mismo de manera más completa y satisfactoria.

Por todo esto, surge la idea de diseñar GSnort.

a. Un vistazo a GSnort

GSnort es una respuesta a esas carencias que Snort tiene. Carencias que se orientan más a la interacción entre el mismo sistema y su administrador, ya que, al no tener una interfaz de usuario amigable, hace un poco áspera dicha interacción y conllevan a ciertas desventajas para el administrador de la red.

GSnort es todo un sistema que permite interactuar de manera más amigable y transparente[10] con el sistema Snort. Permite realizar varias tareas, dentro del contexto de Snort, que le facilitarán el trabajo de administración. Dichas tareas pueden englobarse, a reserva de que más adelante en el documento se detallen, en las siguientes:

[9] Que el usuario del sistema planteado se sienta cómodo y satisfecho con el uso del mismo.
[10] El administrador hará lo básico y el sistema GSnort se encargará de la parte difícil y tediosa. Asegurando un confiable y seguro desarrollo de dicha parte difícil y tediosa para que el administrador no se esté preocupando por las fallas que pueda cometer.

Administración de la configuración de Snort. Configuración de Snort de manera fácil y dinámica. Creación y manipulación de reglas, variables, plugins, instrucciones de preprocesador y módulos de salida de Snort. En otras palabras, configuración total de manera sencilla del sistema Snort.
Manipulación de su funcionamiento Arranque y detención del sistema de manera sencilla y transparente para el administrador del mismo.
Trabajo en tiempo real Detección constante de las salidas de Snort. Recepción de datos. Recepción de datos generados por Snort cuando el administrador asi lo solicite. Aviso de alertas. En cuanto se genere una alerta, GSnort dará aviso al administrador, permitiendo a este último tomar medidas convenientes.
Posibilidad de actuar ante alertas Ejecución de comandos del sistema para que el administrador pueda realizar acciones directas sobre el sistema operativo.
Manipulación de archivos Capacidad de manipular los archivos que existan dentro de Snort. Podrá realizar cualquier operación con dichos archivos.
Trabajo en red Trabajo de manera remota, para que el administrador no esté obligado a estar trabajando en la computadora donde se encuentra el Snort.
Lectura de registros Permitir al administrador poder analizar archivos de registro de Snort de manera dinámica, buscando por patrones dentro de los mismos archivos.

Esta y otras capacidades son las que caracterizan el sistema GSnort.

La estructura con que GSnort le permite no consumir gran cantidad de recursos[11], esto permite que GSnort pueda trabajar en computadoras de bajos recursos.

b. Funcionamiento de GSnort

Para entender el funcionamiento del sistema GSnort hay que observar la manera en que está diseñado, y después ver las capacidades del mismo y sus extensiones.

Básicamente, el estudio del funcionamiento del sistema GSnort se puede dividir en varias partes.

[11] Recursos de la computadora en donde se encuentra instalado, memòria ram, procesador, entre otros.

Estructura del sistema
El sistema GSnort tiene la siguiente estructura:

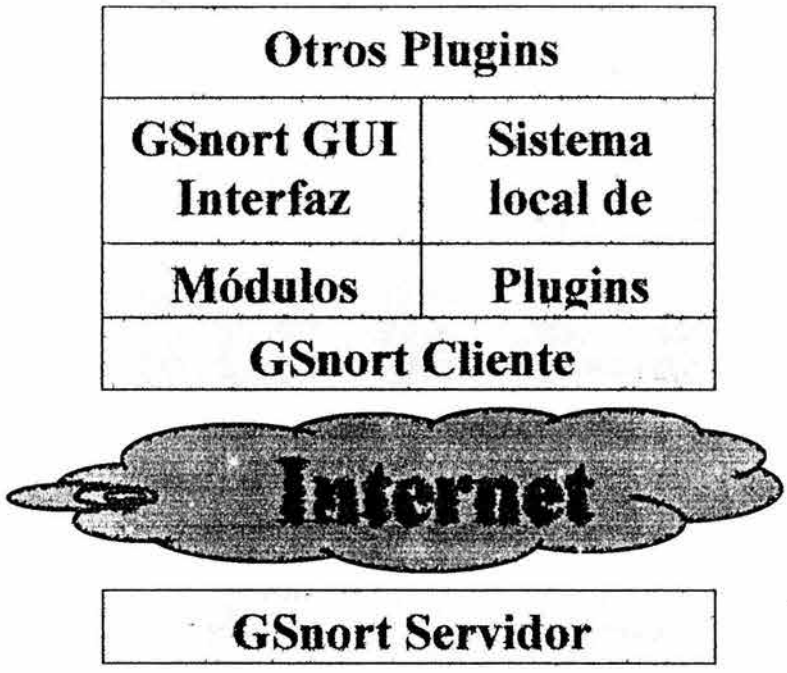

Figura 5-1. Estructura del sistema GSnort

La estructura del sistema se divide en dos partes importantes, una que trabaja del lado del servidor para proveer los datos e interactuar de manera directa con el sistema Snort, y la otra que trabaja del lado del cliente para interactuar de manera dinámica y remota[12] con Snort.

Esto con la finalidad de hacerlo ligero y de bajo consumo de recursos. Cada una de las partes del diagrama del sistema expresado arriba se detallan en las siguientes secciones.

Con esta arquitectura GSnort logra separar la parte visual, lo que es la interfaz gráfica de usuario, del corazón del sistema, de tal manera que aún cuando el administrador de Snort no quiera trabajar con la interfaz el sistema GSnort esté monitorizando las actividades de Snort de manera remota.

Así, la parte GSnort Servidor, al estar siempre corriendo[13], siempre esta captando los datos de Snort y los envía cuando sea necesario[14]. Así mismo, el programa cliente, cuando se ejecuta, le puede indicar al programa servidor, por medio de una instrucción dada por el administrador, que le envíe los datos que Snort está generando. Provocando con esto que el sistema trabaje solamente cuando el administrador se lo

[12] Por medio de Internet desde otra computadora.
[13] Ejecutándose.
[14] Cuando el programa cliente, a través de una instrucción, se lo indique.

indique, y en caso contrario entra en un estado de 'espera' hasta que el administrador le indique que salga del mismo.

A continuación se detalla un poco el funcionamiento del la parte del sistema llamado 'GSnort servidor'.

GSnort Servidor

Este se encarga de mantener la comunicación con el sistema Snort para poder recibir datos, enviarle datos, manipularlo y administrarlo, entre otras tareas.

Su función primordial es el de proveer a los diferentes programas clientes[15] una interfaz de comunicación entre dicho programa cliente y el sistema Snort.

Consta de 6 partes: GSnort Log (Maneja archivos de registro), GSnort Core (Envía instrucciones a Snort), GSnort Conf (Manipula archivos de configuración de Snort), GSnort Command (Recibe comandos del cliente y los ejecuta), GSnort Out (Manda datos de salida) y GSnort Command Stack (Almacena comandos que llegan a GSnort Servidor).

La estructura que forman todas estas partes juntas es la siguiente:

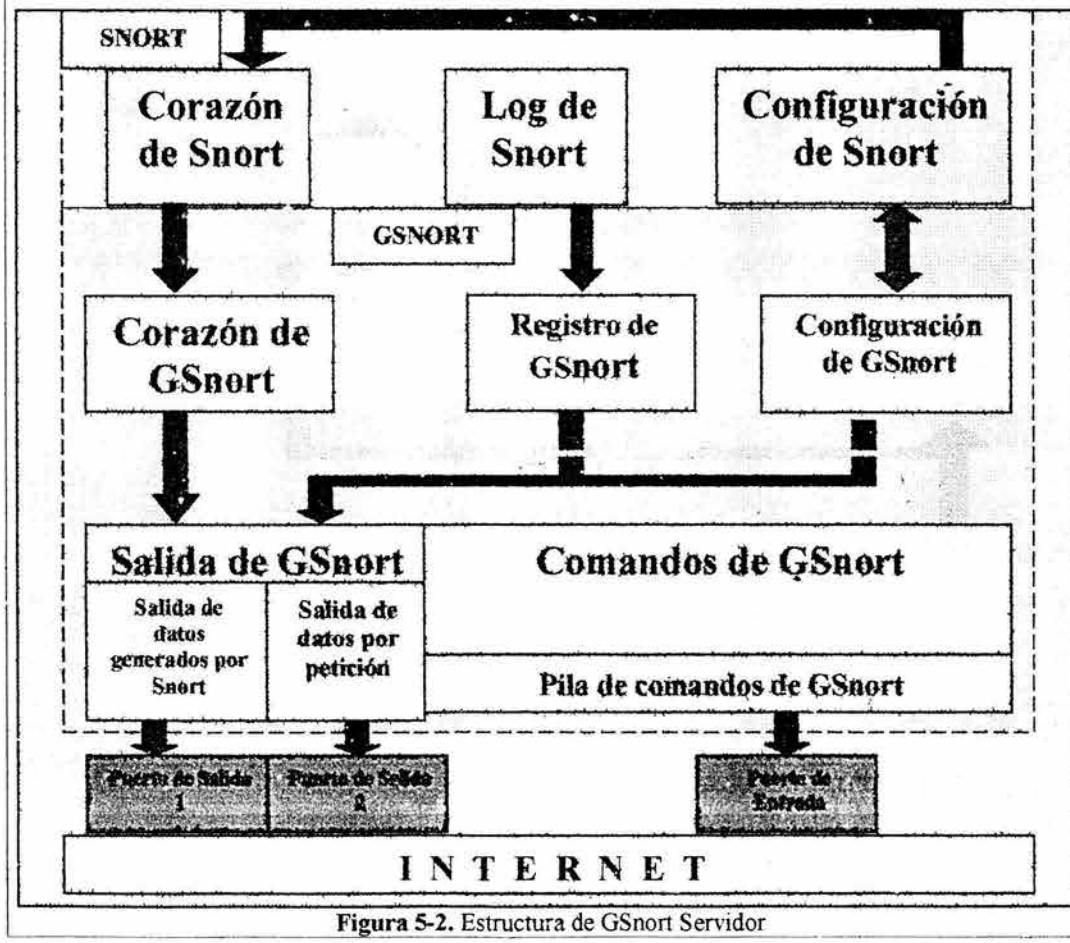

Figura 5-2. Estructura de GSnort Servidor

[15] Interfaces de usuario remotas.

Como se puede observar, el GSnort Servidor consta de varias partes:
- Snort
- GSnort Servidor

En cada una de estas existen módulos internos, los cuales, como se puede observar, se listan a continuación:
- Snort
  - Corazón de Snort
  - Log de Snort
  - Configuración de Snort
- GSnort Servidor
  - Corazón de GSnort
  - Registro de GSnort
  - Configuración de GSnort
  - Salida de GSnort
  - Comandos de GSnort
  - Pila de comandos de GSnort
  - Puertos de entrada y salida de GSnort

El detalle de cada uno de dichos componentes se encuentra en el apéndice D (Componentes de GSnort Servidor).

En cuanto al funcionamiento del lado del cliente se tiene lo siguiente: -

GSnort Cliente

Mantiene comunicación entre el servidor donde se encuentra GSnort Servidor y la computadora donde se encuentra el cliente que desplegará los resultados, mantiene al cliente en comunicación con Internet, de proveerle a la interfaz de usuario los datos que son enviados desde el servidor, de enviar los datos del cliente hacia el servidor, entre otras.

Dentro del diagrama que describe los componentes del sistema GSnort presentado arriba en este documento, como se puede observar, es la primera capa que se encuentra después de Internet, esto hace que cualquier dato que salga o entre al cliente tiene que pasar por este componente. Esto provoca que la interfaz de usuario tenga comunicación con este componente para poder desplegar los datos que el administrador del sistema GSnort quiera. Esta arquitectura permite que este componente trabaje de manera independiente de los otros.

Al trabajar de manera independiente de los otros componentes, permite que el sistema GSnort que se encuentra del lado del cliente este recibiendo datos constantemente sin que se desplieguen dichos datos en alguna interfaz de usuario.

Lo anterior permite que se puedan implementar diferentes interfaces de usuario para cada cliente. Lo único necesario para dicha interfaz de usuario es que tome los datos de este componente y los despliegue de acuerdo a la configuración de dicha interfaz. Esto da flexibilidad para aquellas personas que quieran desarrollar alguna interfaz de usuario especializada para algún cliente en particular.

La arquitectura de este componente es muy sencilla, ya que lo único que realiza es recibir los datos, ya sean instrucciones, datos procesados o datos generados por el sistema Snort, y almacenarlos hasta que la interfaz los solicite, o, en caso de que la interfaz no esté en funcionamiento, solamente recibe los datos y no los almacena.

El siguiente diagrama presenta la arquitectura con que este componente trabaja:

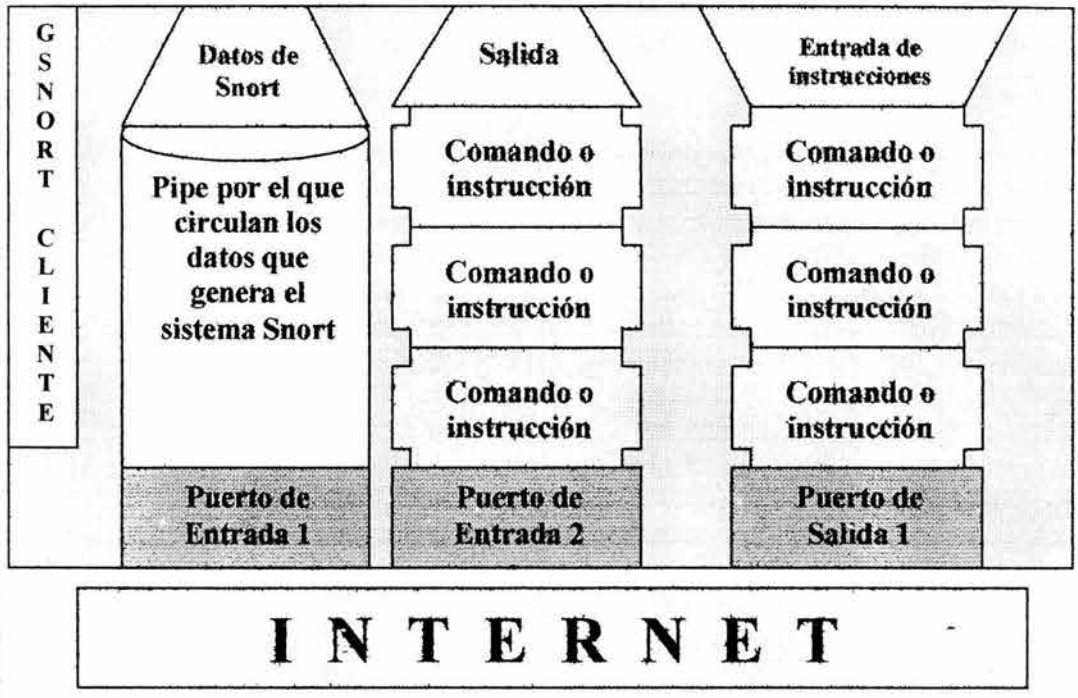

Figura 5-3. Estructura de GSnort Cliente

Se compone de varias partes, dos puertos de entrada y uno de salida (En fondo gris), dos colas de espera de comandos (en fondo celeste), un 'pipe' por el cual solamente circulan los datos que llegan al puerto (en fondo rosa), dos interfaces de datos de salida del componente (en fondo amarillo) y una interfaz de datos de entrada al componente (en fondo naranja). Cada uno con su respectiva función y trabajando de manera independiente de los demás.

Como se puede observar, el GSnort Servidor consta de una parte:
- GSnort Cliente

En cada una de estas existen módulos internos, los cuales, como se puede observar, se listan a continuación:
- GSnort
    - o Puertos de entrada
    - o Puertos de salida
    - o Pipe de datos
    - o Interfaz de datos de salida
    - o Interfaz de datos de entrada
    - o Cola de espera de comandos

Cada uno de las partes de este componente se detallan en el Apéndice E (Componentes de GSnort Cliente).

En cuanto a los módulos y plugins, que es otra parte muy importante del funcionamiento de GSnort, se detallan a continuación:

Módulos y Plugins

Los módulos y los plugins en GSnort forman una parte muy importante dentro del funcionamiento del mismo, ya que a través de ellos se le puede dar un tratamiento extra a los datos, o bien se puede aumentar la funcionalidad del mismo GSnort.

La interfaz, por si sola, como se explicará más adelante, no tiene ninguna funcionalidad, sino que se basa en los módulos y los plugins para adquirir toda su funcionalidad que le caracteriza y distingue. Sin estos, GSnort no tendría sentido, ya que no podría interactuar de manera dinámica y ágil con el administrador de GSnort.

Un módulo está destinado a brindarle otras funciones diferentes a las estipuladas en la versión primera de GSnort. Simplemente realiza operaciones útiles al administrador referentes a la interfaz, esto quiere decir que está dedicado a la interacción con el administrador. Generalmente va acompañado de un plugin, pero no siempre lo necesita, y, cuando va acompañado de un plugin generalmente este último se encarga del proceso de datos, mientras que el módulo se encarga de la presentación de los mismos. Se puede agregar nuevos módulos mediante la interfaz de usuario, o mediante los archivos de configuración.

Un plugin tiene la función de trabajar con los datos que llegan a la interfaz de usuario, o bien, que salgan de ella. Su función se orienta mucho a la manipulación de los datos. Un plugin, al igual que un módulo puede agregarse a GSnort mediante la interfaz de usuario o mediante los archivos de configuración.

Cuando un plugin o un módulo es agregado mediante la interfaz de usuario, ésta se encarga de modificar los archivos de configuración necesarios y de realizar los ajustes necesarios en la configuración de GSnort para que en su funcionamiento incluya el nuevo elemento. Por esta razón, si un módulo o un plugin es agregado mediante la interfaz de usuario, uno solamente le tiene que dar la ruta en la que se encuentra dicho módulo y dicho plugin, y la interfaz se encarga de agregarlo.

Contrario a lo anterior, agregar módulos o plugins directamente en los archivos de configuración resulta inseguro ya que el administrador que los agregue tiene que tener la plena certeza de se encuentra haciéndolo bien, en caso contrario no podrá cargar dicho módulo o plugin cuando levante el servicio GSnort. Ya que la interfaz de usuario, ya tiene programado la manera en que se tiene que guardar dichos cambios, es muy recomendable que el administrador realice esta operación mediante la misma.

GSnort cuenta con una serie de módulos que le ayudan a realizar las tareas básicas del mismo sistema. Enviar instrucciones, recibir datos, leer datos enviados por el Corazón de GSnort en el servidor, leer los diferentes tipos de archivos, crear cualquier componente de los archivos de configuración, controlar los componentes de los archivos de configuración, entre otras.

A continuación se explican algunos de los módulos con que cuenta GSnort:

Leer datos de GSnort Core Despliega en pantalla con un específico formato los datos que llegan a GSnort Cliente provenientes del GSnort Servidor. Cada formato con que se despliegan dichos datos implica que un módulo diferente está actuando sobre esos datos.
Enviar instrucciones Toma los datos que se desean enviar, los empaquetar de la manera en que GSnort Servidor los entienda, los prepara para el envío, y por último los envía.
Leer los diferentes tipos de archivos Lee los diferentes tipos de archivos, ya sean de configuración, registro u otro, que GSnort Servidor envía. A través de este, el cliente puede observar los archivos que GSnort Conf y GSnort Log le envían.
Crear componentes de los archivos de configuración Crea las reglas, variables, y demás componentes necesarios para la configuración correcta de Snort. Cuando el usuario se encuentra armando[16] todos los componentes que él desea para la configuración del sistema Snort, este módulo es el encargado de recibir los datos que el administrador le da a la interfaz de usuario, los analiza[17], y en caso de que estén bien formados, se los manda al módulo encargado de almacenarlos, en caso de que no estén bien formados le envía al administrador un mensaje de error indicándole donde cometió tal.
Controlador de componentes de los archivos de configuración Este módulo recibe los componentes de configuración empaquetados provenientes del módulo de creación de componentes de configuración, los almacena[18] bajo una estructura específica y ordenada, y accede a ellos.

Así como existen los módulos mencionados arriba, también existen otros módulos que se encargan de otras tareas, así como también existen plugins dedicados a tareas específicas del sistema GSnort.

Cuando se habla de un software en donde el o los usuarios de dicho software interactúan mucho con aquel, hablamos de que dicho software cuenta con una interfaz gráfica de usuario, la cuál juega un papel muy importante para dicha interacción. Otro de los roles que juega la interfaz gráfica de usuario es hacer más fácil la labor de administración o manejo de dicho software, por lo que pasa a ser una de las partes más

[16] Creando cada componente en los archivos de configuración (Reglas, variables, módulos, etc.).
[17] En cuestión de sintaxis, semántica. Analiza todos y cada uno de los componentes que el administrador crea de acuerdo a el proceso de análisis estipulado para cada tipo de componente.
[18] Al almacenarlos los guarda en memoria para tenerlos disponibles de manera ágil.

importantes dentro de la interacción entre el humano y la computadora en el contexto del software.

A partir de lo anterior podemos deducir que la interfaz gráfica de usuario en GSnort es muy importante y juega un papel igual de importante. Incluso se podría decir que juega un papel todavía más importante debido a que el objetivo de GSnort es proveer a los usuarios del sistema Snort un software que les permita interactuar con dicho sistema, con lo cuál se infiere que dicho software tiene que tener una manera interactiva de relacionarse con Snort. Y dicha manera interactiva consiste en una interfaz gráfica de usuario que le permita configurar, administrar y controlar el sistema Snort de una manera fácil y dinámica.

Interfaz de usuario

La interfaz gráfica de usuario fue diseñada para que el administrador tenga la facilidad de navegar en ella con comodidad, eficiencia y a gran nivel de detalle, para que se sintiera cómodo porque es uno de los principales objetivos de una interfaz gráfica de usuario. Estas características permite al administrador trabajar de manera tranquila, sin ocasionar problemas relacionados con falta de información o no encontrar algo dentro de la misma interfaz y sin ocasionarle mucha impaciencia.

La eficiencia se ve reflejada en lo fácil que le es al administrador encontrar cada una de las funciones que dicha interfaz le permite. Así como la rapidez con que la interfaz realiza dichas funciones.

El gran nivel de detalle se refiere a que cada una de las partes que definen la interfaz tiene su ayuda para guiar al administrador. Aparte que cada una de las partes de la interfaz está diseñada para que el administrador introduzca todos los datos necesarios sin ocasionar que este último se pierda[19] en dicha parte de la interfaz.

La interfaz de GSnort permite al administrador realizar todas las tareas de configuración, control y administración del sistema Snort de manera remota. Para cada una de dichas funciones tiene una pantalla específica y detallada. Contiene interfaces[20] para generar reglas, variables y cada uno de los componentes de configuración de Snort. Así mismo, contiene interfaces para armar los archivos de configuración de Snort, para desplegar los datos que envía GSnort Servidor, para desplegar los archivos de registro que genera el sistema Snort.

Una de las ventajas que tiene GSnort es que dado que debajo de la capa en donde se encuentra la interfaz gráfica de usuario está la capa de módulos y plugins, uno como administrador puede crear pequeñas interfaces que se acomoden a nuestros gustos y necesidades, ya que la capa de interfaz gráfica de usuario se basa mucho en la capa inferior a ella. De dicha capa obtiene, mediante los módulos y plugins, las pequeñas interfaces dedicadas a atender cada función.

[19] Cuando el usuario no sabe cuál es el funcionamiento de cada una de las partes que conforman la pantalla que se encuentra observando.
[20] Pantallas dentro de la interfaz gráfica de usuario general.

Dentro de las pequeñas interfaces con que cuenta GSnort se encuentran las siguientes:

Creación de reglas, variables y demás componentes de configuración de Snort

Permite al administrador generar una nueva regla de configuración de Snort. Le presenta todos y cada uno de los campos con que cuenta, tanto las de la cabecera como los campos de las opciones, la regla. Aquellos campos que solamente se puedan colocar ciertos valores definidos por Snort, se le presentan a manera de 'combobox'[21] con las opciones posibles para dichos campos.

Esta interfaz se apoya mucho en la interfaz que se encarga de indicarte los componentes de configuración existentes. Ya que en cada campo, dado que se pueden introducir variables definidas previamente por el usuario, cuando uno como creador de la regla se lo indica, despliega la interfaz donde nos indica las variables que ya hemos definido, se elige la deseada y automáticamente se agrega al campo en cuestión. Esto resulta muy útil ya que agiliza el trámite de realización de reglas.

Puede indicar si cada uno de los campos de la regla se encuentra bien formados, y, en caso de no ser así le envía un mensaje de advertencia.

Esta interfaz tiene la capacidad, en caso de que se quiera agregar una variable, de indicar si dicha variable se encuentra definida antes que la regla que se está definiendo. Esto ayuda al administrador a formar bien las reglas y ordenar cada uno de los componentes dentro de los archivos de configuración.

Visualización de componentes de configuración del sistema Snort

Permite, mediante el despliegue de una pantalla pequeña, la visualización de todos los componentes que se encuentran declarados dentro de los archivos de configuración.

Generalmente es muy usado por el módulo que genera las reglas, ya que cuando uno construye una regla se puede apoyar mucho en las variables ya declaradas anteriormente, y este módulo, en el momento en el que uno se lo pida, te despliega dichas variables

En este caso, cuando uno llama a la ventana de este módulo, generalmente la manda llamar desde una caja de texto. Una ves que aparece dicha ventana con los valores de todas las variables, uno elige la que desea agregar, oprime 'aceptar' y devuelve el valor de la variable colocándola de manera automática en la caja de texto desde donde se llamó.

[21] Caja de texto extendible que presenta varias opciones.

Creación de archivos de configuración de Snort

Permite al administrador de GSnort ir creando paso a paso los archivos de configuración de acuerdo a como él mismo, el administrador, crea conveniente.

Ayuda a controlar los archivos que se van creando, los que se borran, así como el llenado de cada uno de dichos archivos.

Cuando se edita el archivo principal de la configuración de Snort, uno puede ir agregando los componentes necesarios. Dado que en dicha configuración puede uno colocar el componente 'inlude[22]', en el momento en que lo agrega, el módulo, en su manejador de archivos, agrega una instancia de dicho archivo agregado, para que posteriormente le avise al administrador que el archivo debe de ser llenado.

Visualización de los archivos de registro de Snort

Permite desplegar los archivos de registro, que envía GSnort Servidor, de manera detallada al administrador para que este último los pueda ver.

Puede darle cierto formato, dependiendo del gusto del administrador, a la información de esta índole enviada desde GSnort Servidor.

Arranque del sistema Snort

Interfaz donde le presenta al administrador todas las banderas de funcionamiento que se le pueden brindar a Snort cuando se arranca. Permite al administrador construir la instrucción, que se le dará a la línea de comandos de Snort, para arrancar el funcionamiento del sistema Snort.

Ayuda al administrador a comprobar si la línea que se le enviará a GSnort Servidor se encuentra bien formada, y, en caso de que no, le avisa de los errores.

En el caso de las banderas de funcionamiento a las cuáles solamente le podemos enviar ciertos valores ya predefinidos por Snort, estę módulo le presenta al administrador dichos valores en un 'combobox' para que elija el deseado.

Visualización en tiempo real de datos generados por el sistema Snort.

Encargado de conectarse al 'pipe' de llegada de datos producidos por Snort y desplegarlos en la interfaz gráfica de usuario.

Existen varios plugins, que trabajan con este módulo, que cambian el formato de despliegue de los datos, con lo cuál el administrador tendrá diferentes puntos de

[22] Agrega un archivo a los archivos de configuración.

vista para dichos datos provenientes de GSnort Core.

Estos y otros muchos son los módulos con los que cuenta GSnort. Cada uno de los módulos trabaja, en su mayoría, apoyándose en uno o varios plugins, por lo que se puede decir que los dos van tomados de la mano en el sistema GSnort.

Una de las ventajas de esta interfaz que cuenta con un módulo que permite agregar más plugins y módulos de manera correcta, con lo que hace todavía más funcional a GSnort. Aunque aquí hay que tener cuidado porque los módulos y plugins tienen que construirse bajo un estándar que entiende GSnort, de otro modo no los entenderá y no los cargará. Vale la pena aclarar que si el módulo o el plugin no se encuentran bien formados y detecta eso en el momento en el que los está agregando, no los agrega e indica el error que GSnort vio en dichos módulos. En caso de que no los detecte en ese momento, sino que los detecte hasta que se este cargando todos los módulos y plugins, en el caso de que este alguno mal no lo carga, le indica al administrador mediante un mensaje cuál resultó ser el problema y sigue con los demás.

Estos, los módulos y plugins, son la parte medular de la interfaz gráfica de usuarios, ya que en su mayoría son pequeñas interfaces hechas con la finalidad de alguna función específica.

Esta parte de GSnort, la interfaz gráfica de usuario, es la única de todo el sistema GSnort con la que tiene interacción, de manera directa, el administrador. Pero, a través de ella, puede tener todo el control del sistema GSnort completo, así como del sistema Snort a través de GSnort Servidor.

Sistema de archivos local

Generalmente cualquier software tiene una serie de archivos que utiliza para diversos fines, ya sea para su configuración, sus registros de actividades, registros de errores o de cualquier otra índole, archivos de imágenes que usa dentro de la aplicación, entre otros tipos de archivos. Dicho conjunto de archivos son necesarios para que el software en cuestión funcione correctamente y como salida de datos de la aplicación.

En el caso del sistema Snort, cuenta con archivos de configuración[23], archivos de registro de datos generados[24], y otro tipo de archivos. Todos estos archivos son necesarios dentro del contexto del sistema Snort, cada uno tiene una función específica, son parte del sistema.

GSnort también cuenta con un sistema de archivos que utiliza para diferentes fines. Archivos de configuración que definen valores de variables utilizadas durante su funcionamiento, indican los plugins y módulos instalados, así como su funcionamiento, indican los puertos de entrada y salida, entre otras cosas; así mismo cuenta con archivos

[23] Generalmente se almacenan en el directorio de instalación, dentro del directorio llamado 'conf'. Aunque Snort permite que se tengan archivos de esta índole en otro directorio, incluso fuera del directorio de instalación.

[24] Generalmente se almacenan en el directorio de instalación, dentro del directorio llamado 'log'. Aunque Snort permite que el administrador le indique en que directorio se almacenarán este tipo de archivos, y este puede ser alguno fuera del directorio de instalación.

de registro de operaciones, en los cuales GSnort registra las operaciones que, según los archivos de configuración, tiene que registrar; cuenta también con archivos que se utilizan para darle configuración a los plugins y a los módulos que sean parte del sistema GSnort. Estos archivos y otros más forman parte de GSnort Cliente y GSnort Servidor, cada uno tiene los propios y con sus respectivas características.

Archivos de configuración

Archivos más importantes dentro del sistema de archivos local de GSnort, tanto del Servidor como del Cliente.

Son varios los archivos que se pueden tener, ya que como en el sistema Snort, el archivo principal de configuración puede mandar llamar a otros archivos. De esta manera uno puede tener más ordenada la configuración del sistema.

Los archivos de configuración son escritos en xml. Se utiliza este formato debido a que es fácil de leer por los usuarios, son fáciles de formar, no ocupan mucho espacio en disco duro y son muy manejables. En caso de que el administrador quiera modificar algún archivo sin utilizar la interfaz gráfica de usuario, este puede leer los archivos, y dado que están escritos en xml, se le hará fácil encontrar lo que busca y modificarlo. Y, en caso de que quiera utilizar la interfaz de usuario para eso, pues la misma interfaz lo llevará a través de los archivos para modificar la parte que se desea modificar.

Para ambos caso, los archivos se encuentran en el directorio de instalación del sistema, ya sea GSnort Servidor o GSnort Cliente, dentro del directorio llamado 'conf'. El archivo que GSnort Servidor lee cuando arranca su funcionamiento se llama 'servidor_conf.xml', mientras que el que lee GSnort Cliente se llama 'cliente_conf.xml'. Aquí se colocan todas las instrucciones necesarias para la correcta configuración de los sistemas que forman GSnort, algo que resultaría en una lectura de dicho archivo algo complicada, o bien, desde dicho archivo, ya sea para el Cliente o para el Servidor, se puede mandar llamar a otros archivos para que la configuración se distribuya en varios archivos y le sea más fácil analizar al administrador.

En el caso de GSnort Servidor en estos archivos se indican propiedades como los dos puertos de salida y el puerto de entrada, directorios o rutas de donde se tomarán archivos de configuración, rutas de los archivos que se utilizarán para configurar cada una de las partes de los componentes de GSnort Servidor, entre otras propiedades que GSnort necesita para su correcta configuración.

Para GSnort Cliente, dicho archivo contiene propiedades como el número de cada uno de los puertos de entrada y el de salida, las direcciones ip del host donde se encuentra GSnort Servidor, los directorios o rutas donde se encuentran cada uno de los módulos y cada uno de los plugins, los archivos de configuración de dichos módulos y plugins, archivos donde se registrarán los movimientos de GSnort Cliente, y demás propiedades que GSnort Cliente necesita para su buen funcionamiento.

Para que no haya confusión, cuando el administrador crea por su propia mano algún archivo de configuración, se recomienda que el nombre empiece con 'servidor_'

en caso de que sea parte de a configuración de GSnort Servidor, y 'cliente_' para GSnort Cliente. Esto para e itar confusión entre uno y otro cuando arrancan su funcionamiento.

Archivos de registi o

Utilizados GSnort Servidor y GSnort Cliente para almacenar los movimientos que se realizan en cada una de las partes de GSnort.

El formato en que se almacenan los datos en estos archivos es propio de GSnort, de tal manera ¡ue cuando el administrador pida leer dichos archivos, el sistema entienda su formato.

Estos archivos generalmente, se guardan dentro del directorio llamado 'log', aunque esto puede cambiar si uno cambia la propiedad correspondiente en los respectivos archivos de configuración.

Archivos de configuración de plugins y módulos

Indican a cada uno de os módulos y plugins las propiedades necesarias para el arranque del funcionamiento de cada uno. La ruta de dichos archivos se encuentra especificada dentro de los arcl ivos de configuración.

Otros Plugins

Dentro del sistema GSnort existen otros plugins que, si bien no interactúan con los datos de manera directa, son de gran importancia para la portabilidad del sistema. Están orientados a la interacción entre GSnort Cliente y otras aplicaciones. Es decir, dado que en el mundo del software lo ideal es poder tener comunicación entre varias aplicaciones, esta capa de plugins provee esa capacidad, es semejante a una interfaz para que otras aplicaciones puedan aprovechar la funcionalidad de GSnort.

Básicamente otras aplicaciones pueden tener acceso a GSnort a través de dichos plugins, con lo que pueden estar recibiendo datos desde GSnort para desplegarlos en dichas aplicaciones.

Entre los plugins de GSnort que existen en esta capa están los siguientes:

Lectura de propiedades

Permite a las aplicaciones externas a GSnort ver las propiedades bajo las cuáles GSnort Cliente se encuentra funcionando.

Es importante decir que no todas las propiedades están disponibles para este

plugin, ya que algunas propiedades se ocultan por seguridad.

Lectura de archivos

Lee los archivos de configuración que GSnort Cliente puede modificar.

Dichos archivos son los que utiliza el sistema Snort para su configuración.

Cuando alguna aplicación utiliza este plugin, GSnort Cliente, en caso de no tener dichos archivos, lo pide a GSnort Servidor, y posteriormente se los brinda a la aplicación en cuestión a través del este plugin.

Lectura de datos

Permite leer los datos que el Corazón de GSnort envía. Son los que genera Snort en tiempo real a causa de los paquetes de datos que puedan resultar dañinos para la red.

Con esto, otras aplicaciones pueden tener acceso a estos datos que, en muchas ocasiones, son la parte importante de GSnort.

Así como los plugins explicados arriba, existen otros plugins que permiten a otras aplicaciones adquirir ciertas funcionalidades de GSnort.

c. Ventajas y desventajas del sistema

Este sistema, al igual que cualquier sistema de software, tiene ventajas y desventajas. Algunas ventajas radican en la funcionalidad de GSnort, y, por el contrario, algunas de las desventajas provienen de su portabilidad.

Dado que un sistema tiene su éxito por las ventajas, empezaremos por explicar algunas de ellas:

Capacidad de trabajar de manera remota

Capacidad de trabajar de manera remota, es decir, dado que consta de dos partes, GSnort Cliente y GSnort Servidor, el primero se conecta con el segundo. El segundo se encuentra donde se encuentra el sistema Snort instalado, mientras que el primero puede estar en la misma computadora o alguna otra computadora en otra parte del mundo. La conexión se puede hacer a través de Internet o de intranet.

Las capacidades que tiene son configuración, manipulación y control total del sistema Snort, con lo cuál hace más poderosa esta herramienta.

Capacidad de interactuar con otras aplicaciones

Mediante la arquitectura bajo la cuál fue diseñado este sistema, la capa de plugins que contiene en la parte más externa de GSnort Cliente le permite a otras aplicaciones interactuar con GSnort Cliente como ya se explicó.

La funcionalidad que dichas aplicaciones externas pueden adquirir de GSnort esta restringida a aquellas funciones y datos que no provoquen inseguridad en el funcionamiento de GSnort.

Fácil y entendible configuración

Los archivos de configuración, creados con xml, son fáciles de leer por cualquier administrador. A esto se le une que se puede configurar desde la misma interfaz de manera fácil y dinámica.

En cuanto a la configuración del sistema Snort mediante GSnort Cliente, también ofrece una manera bastante entendible, fácil, dinámica y completa para realizar todos los movimientos necesarios para formar los archivos de configuración del sistema Snort. Esto permite al administrador realizar dichos archivos de manera muy tranquila, sin preocuparse por los errores que pueda cometer, ya que la interfaz le da aviso de dichos errores.

Multiplataforma[25]

El lenguaje de programación con que se hizo GSnort, JAVA[26], permite correr de la misma forma en diferentes sistemas operativos.

Esto le da mucha portabilidad al sistema, ya que tanto GSnort Servidor como GSnort Cliente pueden estar instalados en cualquier sistema operativo, lo cuál no limita la computadora en la que pueda estar instalado cualquiera de las partes de GSnort.

Incremento de funcionalidad mediante plugin y módulos

La capa de módulos y plugins que está dedicada a definir la funcionalidad de GSnort permite que se le agreguen otros módulos y plugins para incrementar la misma.

Se realiza mediante la interfaz gráfica de usuario de manera fácil y dinámica.

Cuando sucede esto, la interfaz se encarga de hacer los cambios

[25] Es soportado por diversos sistemas operativos (plataforma).

[26] Lenguaje de programación orientado a objetos, cuya principal finalidad en sus inicios fue desarrollar un lenguaje para crear aplicaciones para aparatos electrónicos pequeños y caseros. Cuando fue creciendo se expandió a todos los ámbitos de la computación, hasta ahora que se encuentra en aplicaciones de cualquier índole, incluyendo aparatos electrónicos caseros y móviles.

correspondientes a los archivos de configuración, así que esta forma de hacer esta tarea es segura.

Existe otra manera de agregar módulos y plugins, la cuál se refiere a agregar el nuevo componente directamente en el archivo xml de configuración donde se encuentran definidos dichos módulos y plugins. Como ya se explicó, es lógico pensar que cuando se usa esta manera para agregar un nuevo componente existe una gran probabilidad de que exista algún error.

Dividido en dos partes

Servidor y cliente, permite que GSnort trabaje de manera remota y dinámica, ya que estas dos partes trabajan de manera independiente.

Fácil uso de interfaz de usuario

La interfaz de usuario, en todas y cada una de sus partes, es entendible, fácil de usar, completa, y, sobre todo, capaz de guiar los pasos del administrador que la usa.

La capacidad de guiar al administrador quiere decir que le ayuda al administrador a realizar las tareas propias de cada parte de la interfaz. Esto hace que la creación de dichos tareas sea en menos tiempo que lo que es usado normalmente.

Estas son las ventajas más importantes dentro de el sistema GSnort, aunque vale la pena hacer notar que existen otras.

Pero como en todo, no hay nada perfecto, este sistema tiene algunas desventajas:

Necesidad de cantidad de memoria grande

GSnort se construyo en el lenguaje de programación JAVA. Esto tiene la ventaja de que su funcionamiento es multiplataforma. Pero como se sabe, las interfaces gráficas en JAVA todavía no son muy rápidas y necesitan de más memoria que los otros lenguajes de programación para su apto funcionamiento.

Esto nos acarrea la desventaja de la memoria ram, ya que se necesita de más cantidad de memoria para un ágil funcionamiento. Aunado con esta desventaja, las interfaces gráficas de usuario exigen más poder de procesamiento, es decir, un procesador de mayor poder.

Esta es la desventaja más importante que tiene GSnort. Esta desventaja solo se ve reflejada en la interfaz gráfica de GSnort, ya que el corazón de la misma, tanto en GSnort Servidor como en GSnort Cliente, no implica mucha memoria ni poder de procesamiento porque no incluye alguna interfaz. De esto se deduce que esta desventaja se refleja cuando se levanta la interfaz gráfica de usuario.

Como se puede ver, GSnort tiene ventajas y desventajas, como todo sistema de software. Las ventajas son mayores que las desventajas. La elección de uso de este sistema dependerá de las capacidades económicas[27], de hardware[28], y otro tipo de capacidades[29] con que cuente el usuario final del sistema.

d. Sistemas operativos que lo soportan

La ventaja mayor que tiene este sistema es que se encuentra hecho en el lenguaje de programación JAVA. Este lenguaje no tiene mucho tiempo de existencia, se puede usar para cualquier tipo de aplicación, es multiplataforma, alto grado de facilidad de programar, completo, flexible y amplio.

Gracias a esto, GSnort se puede correr en cada sistema operativo que pueda soportar el lenguaje de programación JAVA, y esto depende en gran medida de los desarrolladores de cada sistema operativo.

Entre los sistemas operativos más importantes en donde GSnort puede trabajar de manera correcta están los siguiente:

- Linux, y todas sus distribuciones[30] diferentes.
- Unix.
- Windows

El buen funcionamiento de GSnort, recordemos, depende de que Snort se encuentre instalado en la misma computadora donde se encuentra GSnort Servidor, esto quiere decir que si Snort no puede instalarse en cierto sistema operativo quiere decir que GSnort no funcionará en dicho sistema operativo.

Lo anterior nos lleva a la conclusión siguiente: GSnort trabaja en aquel sistema operativo donde se pueda instalar el sistema Snort y pueda soportar el lenguaje de programación JAVA. En caso contrario no podrá trabajar de ninguna manera.

[27] Para adquirir equipos de cómputo con la suficiente capacidad para soportar el sistema.
[28] Que se cuente con el equipo necesario para soportar dicho sistema.
[29] Ancho de banda amplio en la red que comunica al servidor con el cliente.
[30] Cada una de las versiones que las compañías de software que desarrollan el sistema operativo linux brindan al mercado.

Capítulo 5

Diseño del Sistema GSNORT

Objetivo:

Presentar la manera en que se pensó en el diseño, la arquitectura y en la codificación del sistema GSNORT.

Dentro del desarrollo de un software, las tareas más importantes son el análisis y el diseño del mismo, porque que, partiendo de ahí, se puede pensar en la arquitectura, o las arquitecturas en caso de que sea necesario, que se usará para montar el sistema entero. Posterior a esto, viene otra parte igualmente importante, decidir como se codificará el software.

Cada una de estas partes son muy importantes en el desarrollo completo del software, desde que da inicio dicho proceso hasta su fin, cuando el software ya se encuentra estable.

En este trabajo nos concentraremos en la parte del diseño, de la arquitectura y de la codificación del sistema GSnort.

a. Diseño

El diseño de software se puede definir como lo siguiente:

"Es el proceso de aplicar distintas técnicas y principios con el propósito de definir un producto con los suficientes detalles como para permitir una buena realización física".

Como uno puede ver, sin esta parte dentro del desarrollo de software es muy difícil que el producto sea de calidad.

Tiene varios propósitos, entre los más importantes se encuentran:

- **Construir un sistema que satisfaga determinada especificación del mismo.**
Una ves que se define cada una de las características con que se quiere el software, el diseño nos permitirá detallar, mediante un modelo, cada una de dichas características, permitiéndonos esto ver la mejor manera en que se puede realizar físicamente.

- **Construir un sistema que se ajuste a las limitaciones impuestas por el medio de destino.**
El diseño nos permite limitar las características del software a aquellas que se pide que tenga el mismo, ya que nos permite detallarlo en dichas características.

- **Construir un sistema de calidad.**
Ya que es de las primeras etapas del desarrollo del sistema, constituye una base sumamente importante, y en ocasiones se considera la más importante, para que el software resulte un sistema de calidad. Si esta etapa se lleve de buena manera, cumpliremos con una gran parte para la calidad del producto resultante.

- Construir un sistema que respete los requisitos de rendimiento, utilización de recursos, etc.
El diseño, así mismo, nos ayuda a tomar en cuenta los recursos[1] con que se cuente, y moldear nuestro modelo de acuerdo a dichos recursos. Esto también nos permite implementar técnicas para sobrellevar la falta de algún recurso, en caso de que cuando esté funcionando el software haya dicha falta de recurso.

En resumen, el diseño consiste en construir un modelo o una representación técnica del software, en este caso el sistema GSnort, que se quiere llevar a la realización.

Existen varios modelos que se pueden utilizar en el diseño del software. Cada uno de dicho modelos con diferentes características, los cuáles abarcan casi cualquier tipo de software a desarrollar.

El sistema GSnort se basó para su realización en el modelo orientado a objetos, ya que era el que mejor se adaptaba a las necesidades y requisitos del sistema.

El modelo orientado a objetos tiene varias características, tales como:

- Abstracción de objetos
Cuando uno diseña mediante un modelo orientado a objetos tiene que pensar en objetos, es decir, tratar de abstraer cada uno de los componentes del sistema en objetos, ver cuáles son sus características semejantes y, a partir de allí, realizar un buen diseño.

- Encapsulamiento
Ya que en esta metodología uno ve los componentes y cada una de las partes como objetos, uno debe de encapsular, en clases, cada una de sus características, así como los métodos de su manipulación.

- Modularidad
Esta característica nos permite realizar módulos tan pequeños como uno crea conveniente. Esto quiere decir que cada módulo hará las tareas pertinentes, de tal manera que uno puede asignarle a un módulo tareas de la misma índole.

- Jerarquía
Dado que se puede abstraer los objetos de acuerdo a sus características particulares, uno puede jerarquizar dichos objetos para tener clasificados cada uno de los objetos de acuerdo a sus características particulares.

- Concurrencia
Nos permite ejecutar, de manera aparente[2], varios módulos al mismo tiempo. Ejecutar varios procesos a la ves nos permite distribuir mejor el trabajo.

---

[1] Memoria ram, disco duro, procesador, dispositivos de almacenamiento, dispositivos externos, y otros. Esta parte es muy importante ya que el software trabajará con dichos recursos.

[2] Cuando uno tiene un procesador en la máquina donde instala el software, y dicho software tiene procesos en concurrencia, quiere decir que el procesador los atenderá a todos, les asignará un tiempo de procesador intercalado a cada uno de los procesos, de tal manera que parece que trabajan al paralelo, pero no es así porque en realidad se encuentran trabajando, operación por operación e intercaladas entre los

- **Persistencia**
Los objetos son capaces de mantener el estado por un espacio de tiempo indicado por el programador del sistema. De esta manera, se logra, en muchos casos, la conservación de datos u operaciones.

En el caso de GSnort, utilizamos todas las características anteriores para darle la completa funcionalidad con que cuenta. De esta manera, cada uno de los componentes de GSnort se maneja como un objeto, en el cuál encapsula sus características, métodos para manipular dichas características y realizar operaciones relacionadas con las mismas. Cada módulo se encuentra formado de una serie de objetos, los cuales se pueden observar como pequeños módulos, que, al trabajar al unísono, realizan las tareas que el módulo tiene encomendado. Así mismo, GSnort jerarquiza sus objetos, aprovechando esto para tener un mejor control de los mismos. También utiliza las capacidades del manejo de objetos para ejecutar diversos procesos al mismo tiempo, procesos que permiten hacer que GSnort trabaje de manera más optimizada. Y, por último, utiliza la bondad de la persistencia para almacenar datos necesarios para varias operaciones, con lo cuál asegura el flujo de dichos datos.

Todos y cada uno de los módulos que contiene GSnort Servidor, los cuales se detallaron en el capítulo anterior, en su interior contienen objetos que realizan, cada uno, una tarea específica, y que en conjunción logran la funcionalidad del módulo en cuestión.

Los módulos, al ser objetos, tienen la capacidad, de acuerdo a lo que nos permite el diseño orientado a objetos, de funcionar en paralelo con otro objeto para que estén realizando, cada quién las suyas, las funciones correspondientes.

Un ejemplo claro de esto se ve en GSnort Servidor, cuando llegan varios comandos dirigidos a varios módulos. En el momento en que son redirigidos, cada uno de los comandos a los respectivos módulos para que sean atendidos, empiezan, estos últimos, a trabajar sin fijarse si algún otro módulo se encuentra en funcionamiento, con lo que se logra un trabajo en paralelo, o concurrencia.

Una ves que se diseñó, basándose en las capacidades que debía contener para cumplir con todas sus funciones, el sistema GSnort de acuerdo a la tecnología orientada a objetos, se continuó con la definición de la arquitectura del mismo sistema, parte importante del mismo.

b. Arquitectura del sistema

Esta es una de las partes medulares de todo el sistema GSnort, ya que es la manera en que se organizó el sistema entero. Este es la parte en la que se define la

procesos, de manera secuencial. En caso de que se tengan dos o más procesadores, pues los procesos se reparten entre los procesadores habidos, por lo que en este caso se puede decir que si trabajan en paralelo dichos procesos.

estructura que GSnort tiene. Se buscó hacer el sistema lo más portable[3], óptimo y eficiente posible.

Dado que la estructura es la que marca este tipo de características, portabilidad, eficiencia y grado de ser óptimo, la estructura básicamente se dividió en tres partes fundamentales, Snort, GSnort Servidor y GSnort Cliente.

Figura 6-1. Estructura básica del sistema GSnort

Como se puede observar consta básicamente de tres partes, el sistema Snort, el sistema GSnort Servidor, y el sistema GSnort Cliente (el cual explicaremos porque se repite tanto en la computadora local como en la computadora remota). Cada una de estas tres partes son indispensable dentro de esta arquitectura.

La arquitectura en la cual se basó GSnort, a este nivel, se llama arquitectura cliente-servidor. Esta arquitectura consiste, a grandes rasgos, en un programa que se encuentra trabajando como servidor de datos, operaciones o transacciones, y un programa cliente que se encarga de realizar las peticiones a la parte servidor, y este último le devuelve la respuesta en forma de datos, operaciones o transacciones.

Cada una de las partes tienen las siguientes funciones:

- **Sistema Snort**

Esta se encuentra abarcada por el software, llamado Snort, que se encarga de realizar las funciones de seguridad en redes de computadoras. Genera las alertas,

[3] Que se pueda correr en cualquier plataforma.

los datos, los registros de los paquetes, los mensajes, y todas aquellas operaciones pertenecientes a un Sistema de Detección de Intrusos.

Este software es del que toma todos los datos la siguiente capa de la arquitectura, GSnort Servidor, para mandarlos al cliente cuando este los solicite.

- GSnort Servidor

GSnort Servidor es el intermediario entre el administrador, que se encuentra en un lugar remoto, conectado a través de Internet, y el sistema Snort, encargado de la seguridad de la red como se ha detallado.

Esta parte de la arquitectura es la encargada, a través de cada uno de sus módulos, de adquirir todos los datos del sistema Snort y enviárselos a la parte llamada GSnort Cliente cuando este los solicite de manera remota.

Dichos datos pueden ser los que Snort genera a raíz del análisis de paquetes y generación de alertas y acciones a causa de dichos paquetes, o archivos de configuración, los cuales generalmente son varios, o archivos de registros, los cuales son donde Snort guarda todos los movimientos que su ejecución genera.

Cuenta con 6 módulos:
- Corazón de GSnort
- Registro de GSnort
- Configuración de GSnort
- Comandos de GSnort
- Pila de Comandos de GSnort
- Salida de GSnort

Esta parte del software, al igual que la anterior, no tienen interfaz gráfica de usuarios.

Interiormente, esta parte de la arquitectura tiene otro tipo de arquitectura, se encuentra formada por una arquitectura de módulos, es decir, el funcionamiento es a través de los 6 módulos mencionados arriba.

Existe interacción, intercambio y flujo de datos entre los módulos; esto para satisfacer todas y cada una de las peticiones del cliente. De esta manera los módulos se relacionan entre si para realizar las funciones de GSnort Servidor.

Dicha arquitectura se puede observar, tanto sus flujos de datos (representados por flechas que van de un módulo a otro) y relaciones (representadas, así mismo, por las flechas), como sus módulos (representados por cuadrados con el respectivo nombre en el interior), en la siguiente figura:

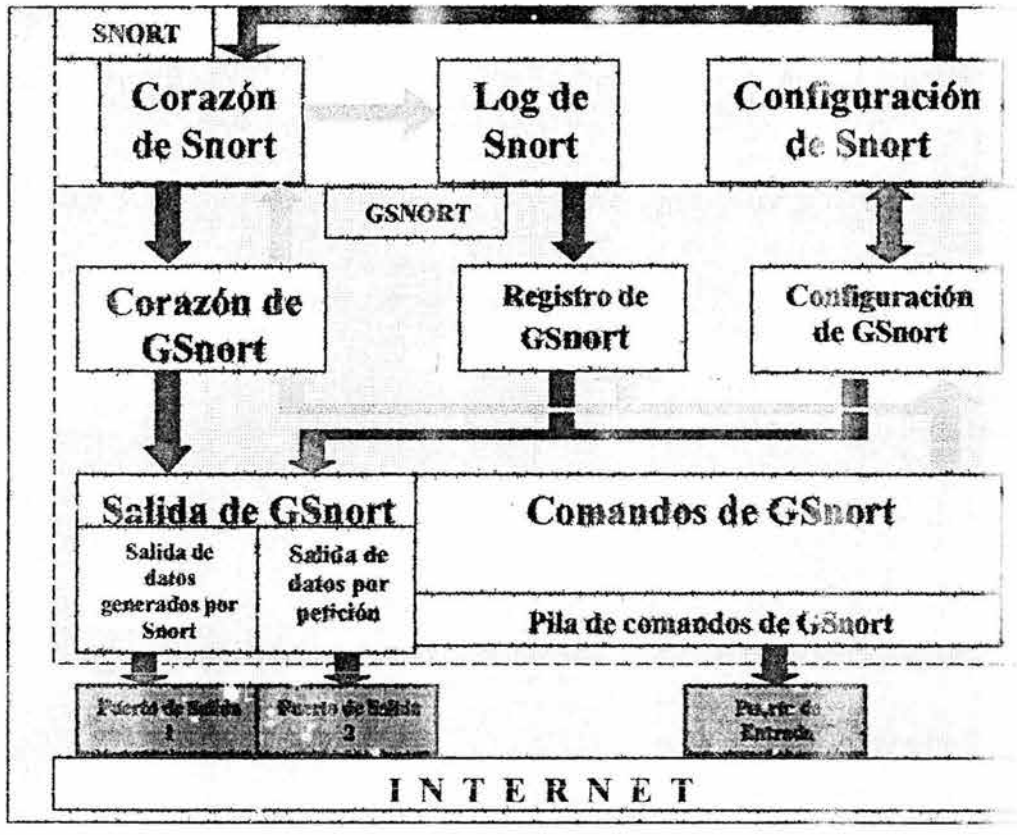

Figura 6-2. Estructura de GSnort Servidor

- **GSnort Cliente**

Esta parte es con la que el administrador va a dirigir el sistema GSnort S... Es la única con la que interactúa, a través de ella realiza todas las tarea... están asignadas.

Interiormente se encuentra formada por una arquitectura de capas, la cuál consta de 6 capas, cada una con sus respectivas características y fun... interactuando algunas con otras. Dichas capas son: GSnort Cliente, M... Plugin, Sistema Local de Archivos, GSnort GUI Interfaz y Otros Plugins.

- GSnort Cliente. Es el puente de comunicación entre el módulo ente... exterior, es decir, Internet.
- GSnort GUI. Es la parte más importante de este módulo ya que es la enc... de presentarle al administrador la interfaz gráfica con la que trabajará y re... todas las funciones necesarias. Aquí, el administrador, realiza la configura... control y administración del sistema Snort.
- Módulos. Encargados de definir cada una de las funciones que... administrador puede palpar en la interfaz gráfica. Se dedican a dar...

funcionalidad a la interfaz mediante pequeñas módulos dentro de la interfaz de usuario.
- Plugins. Son los que generalmente auxilian a los módulos. Generalmente los módulos son los encargados de darle presentación a la tarea que realiza un plugin.
- Sistema local de archivos. Archivos para configurar a GSnort Cliente. Fáciles de leer para el administrador, escritos en XML.
- Otros plugins. Brindan comunicación a GSnort Cliente con otros programas externos al mismo. Esto para que no sea una aplicación invisible y pueda transmitir los datos que ella misma despliega. Estos plugins se comunican con la interfaz gráfica de usuarios a través de una interfaz de esta última.

Dicha arquitectura a continuación se presenta:

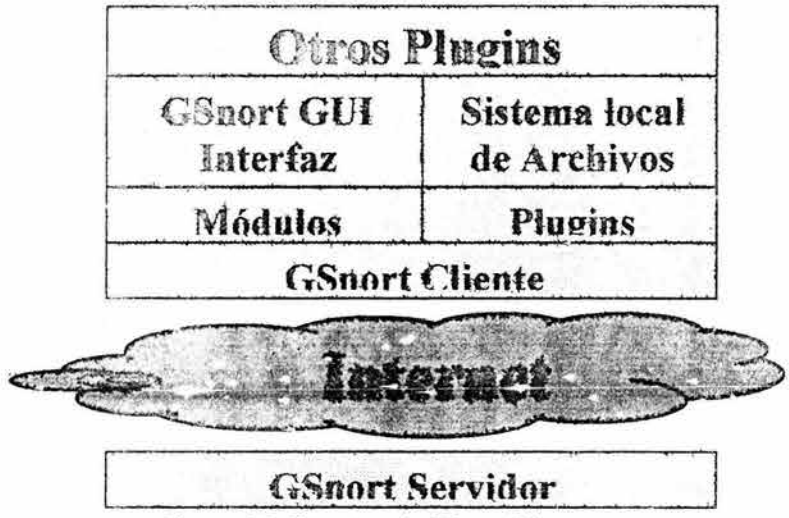

Figura 6-3. Estructura de GSnort Cliente

Por último, esta parte de la arquitectura se repite tanto en la computadora local como en la computadora remota, esto se debe a que esta parte puede estar instalado en la misma computadora en al que se encuentra GSnort Servidor, la única diferencia es que no se necesitaría de Internet para comunicarse con aquel.

c. Codificación

En cuanto a la codificación, cuando se realiza un software es importante decidir de manera correcta cuál lenguaje de programación se va usar, ya que de esa decisión dependerá que el desarrollo y la implementación se compliquen o se simplifiquen.

En el caso de GSnort se utiliza el lenguaje de programación orientado a objetos JAVA, ya que este lenguaje nos permite, de una manera poco difícil, implementar toda la arquitectura que se plantea para este sistema.

JAVA nos brinda muchas ventajas con respecto a los demás lenguajes de programación para este tipo de software, entre ellas podemos hacer mención de las siguientes:

- **Lenguaje multiplataforma**
Esto quiere decir que uno realiza sus programas, los compila bajo el sistema operativo en que se trabaja, y los archivos compilados corren en cualquier otro sistema operativo que soporte el lenguaje de programación JAVA. Esto nos permite realizar una aplicación que cumpla con una de sus principales características: la portabilidad.

- **Manejo de objetos**
El lenguaje de programación JAVA nos permite una implementación de objetos muy sencilla y manejable. Lo cual nos da ventaja para concentrarnos en la arquitectura que se plantea.
El manejo de lo objetos en este lenguaje de programación permite todo lo que el diseño orientado a objetos exige: concurrencia, modularidad, jerarquía, encapsulamiento, etc.

- **Fácil implementación de la arquitectura planteada**
Dado que la arquitectura que se presenta es algo compleja, se usa este lenguaje de programación porque facilita en gran medida la realización de cada uno de los módulos que pertenecen al sistema GSnort.

- **Librerías útiles para las diferentes tareas de GSnort**
Cuenta con una gran variedad de librerías útiles para diferentes ámbitos de la computación, las cuales, muchas de esas, son útiles para la realización del sistema GSnort.
Dentro de las librerías más importantes de JAVA utilizadas para la realización de este software se encuentran las siguientes: SWING[4], JAVA XML[5], y JAVA NET[6].

Otra de las tecnologías que se usa para la realización del sistema GSnort es XML, el cual es una manera de transportar datos de manera fácil, legible y sencilla. Suele utilizarse mucho para realizar los archivos de configuración de muchos de los productos de software que las empresas colocan en el mercado. Es fácil de construir, leer, y muy manejable.

Pues GSnort no es la excepción, los archivos de configuración se encuentran hechos en este formato. Esto simplemente para tener una manera sencilla de manejar la configuración de GSnort.

[4] Librería que es útil para realizar interfaces gráficas de usuarios.
[5] Librerías para manipular archivos escritos en XML.
[6] Librerías para poder comunicarse a través de Internet o de una Intranet.

Conclusiones

A lo largo de este trabajo hemos recorrido un poco el mundo de la seguridad en los sistemas de cómputo, área de la computación que comúnmente es llamada seguridad informática. Hemos visto sistemas operativos que trabajan en red. Dimos un recorrido por algunos aspectos que se tienen que tomar en cuenta dentro de la seguridad en los sistemas de cómputo, así como las herramientas, detalles y cultura que nos pueden ayudar a mantener dicha seguridad.

Analizamos un tipo de software, llamado 'detectores de intrusos', y vimos que son programas que nos auxilian para mantener la seguridad en nuestros sistemas de cómputo. Así mismo vimos como funcionaban, los tipos que hay, ventajas y desventajas de los mismos. Por último, se mencionó algunos de los productos que existen en el mercado que realizan esta tarea, así como algunas de sus características.

Yendo a un nivel más específico, llegamos al análisis del Sistema de Detección de Intrusos llamado Snort. Vimos sus características, su funcionamiento, sus ventajas y sus desventajas. Se vio que era muy buen software pero que no tenía una interfaz gráfica que permitiera al administrador del sistema interactuar de manera dinámica con el sistema, lo cual, dada la manera de funcionar de Snort, se analizó y se llegó a la conclusión de era una desventaja.

Y finalmente, ante dicha desventaja que presenta el Sistema de Detección de Intrusos llamado Snort, se presentó el diseño de una solución.

Solución que consta de un software que le permita al administrador del sistema Snort controlarlo, configurarlo y administrarlo con dos ventajas importantes, la primera es que lo podrá hacer de manera gráfica, dinámica e interactiva, y la segunda es que lo podrá realizar de manera remota.

GSnort es una aplicación completa, con una arquitectura que le permite tener muchas capacidades, adaptable a las necesidades de las tareas del administrador, robusta, portable y con otras características.

Se encuentra hecho con el lenguaje de programación JAVA, lo cual lo hace portable, completo y seguro. Aunque esto también tiene algunas desventajas como el que usa más recursos que si se hiciera con otros lenguajes de programación y el cliente es pesado[1] debido a su interfaz gráfica de usuario[2].

Haciendo una comparativa entre las ventajas y las desventajas que tiene este producto, uno puede ver que las ventajas llevan el camino ganado por sobre las desventajas, por lo que uno puede fácilmente elegir por el uso de este software tomando en cuenta que su utilidad resulta muy extensa y conveniente.

GSnort le facilita el trabajo a los administradores de red en caso de que usen el sistema Snort. Inclusive, si no son administradores de red, si solamente son usuarios de Snort, este software les facilita en gran medida el trabajo.

[1] Necesita de más recursos de la máquina que otras aplicaciones comunes.
[2] Se dice que las interfaces gráficas de usuario en JAVA son todavía algo lentas, aunque esto depende mucho de la máquina donde se este ejecutando dicha interfaz.

Por último, GSnort se diseñó para complementar las capacidades del Sistema de Detección de Intrusos Snort y no para competir con él, simplemente busca ser una herramienta útil en la búsqueda de la seguridad informática y que facilite la interacción entre el administrador y el sistema Snort, sin interrumpir su excelente labor como detector de intrusos.

Con todo lo que hemos visto y partiendo del diseño del software que propusimos en este trabajo, se puede observar que todos los objetivos han sido satisfactoriamente cumplidos.

Por otro lado, GSnort, de acuerdo al diseño, está hecho para que en un futuro pueda implementarse para otros Sistemas de Detección de Intrusos que no sean Snort. Esto es debido a que en su configuración, como lo vimos a lo largo de este trabajo, se hace a través de archivos de texto. Otra de las ventajas de este sistema son los plugins o módulos que se le pueden agregar, con esto se puede dar más funcionalidad para trabajar con aquellos Sistemas de Detección de Intrusos con los que trabaje.

Apéndice A

Presentación de imágenes de algunas partes del prototipo de la Interfaz de Usuario

En este apéndice se presentan algunas imágenes del prototipo de la interfaz gráfica de usuario del sistema GSnort. Este prototipo se construyó para hacer notar la facilidad que brindará al usuario del mismo para la configuración y administración en general del sistema Snort.

Vale la pena recalcar que solamente es un prototipo, con lo cual se quiere extender el entendimiento del funcionamiento de la interfaz gráfica de usuario, y que en el momento de la implementación se tendrá que detallar en la cuestión visual, es decir, se tendrá que realizar de manera más atractivo para que la facilidad para el usuario final sea mayor.

La manera en que se presentan las imágenes en este apartado es dando una explicación, la cual se buscará ser lo más detallada posible, de la misma.

En la primera sección se presentarán imágenes de la interfaz de usuario que se utiliza para la creación de reglas de configuración del sistema Snort.

Las primeras 4 figuras que se presentan son similares, ya que hablan de la manera en que el usuario ingresa valores de la regla. Dichos valores son las acciones de la regla, el protocolo de cada regla, el operador y las opciones de la regla.

Estas imágenes muestran la manera en que al usuario se le facilita dicha tarea. Estas partes de la interfaz gráfica tienen algunas características en común, las cuales se detallan a continuación.

1.Campo de opción. En este campo de texto se desplegará la opción que sea elegida por el usuario. Lo recomendable es que el usuario no escriba nada en esta parte de la interfaz, sino que mediante las flechas elija la opción deseada, esta característica se detalla más adelante.
2.Cuadro de posibles opciones. En este cuadro se presentan las posibles opciones que el usuario tiene referente a la parte de la interfaz en que se encuentra. Este cuadro le permitirá al usuario tener menos posibilidad de error, ya que sólo podrá elegir las opciones posibles.
3.Título descriptivo. Esta parte le muestra al usuario, mediante una pequeña descripción de tres o cuatro palabras a manera de título, el nombre de la parte de la regla que se está editando.
4.Indicador de elemento. Esta barra, con fondo azul y letras blancas, indica al usuario cuál de las opciones es la que seleccionará. Esta barra azul con letras blancas resalta sobre las otras opciones para llamar la atención de los usuarios e indicarlo lo que ya se dijo.
5.Mensajes descriptivos. En este cuadro se le muestra al usuario un pequeño mensaje de tres o cuatro líneas que le indica una pequeña descripción de la opción que en ese momento está seleccionada.

A continuación se presentan las figuras correspondientes:

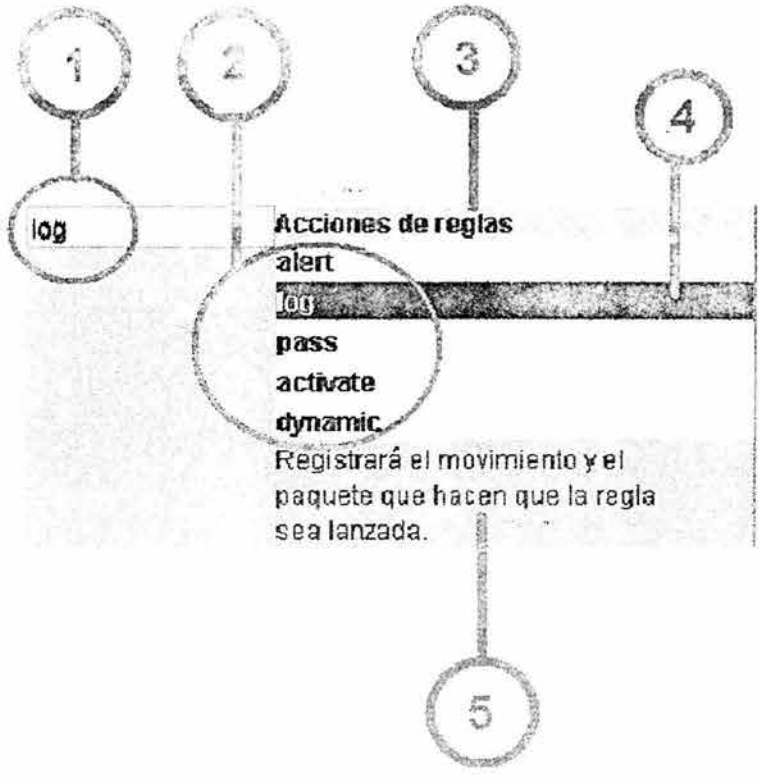

Figura 1. Campo para la introducción de la acción de la regla.

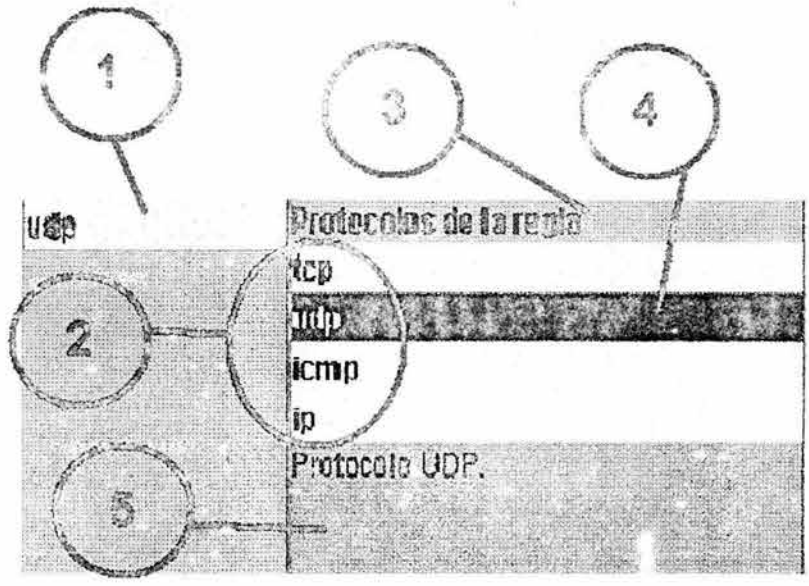

Figura 2. Campo para la introducción del protocolo de la regla.

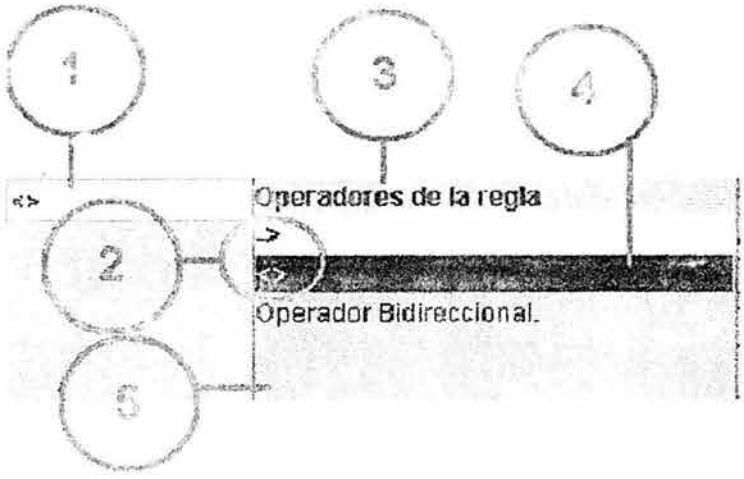

Figura 3. Campo para la introducción del operador de la regla.

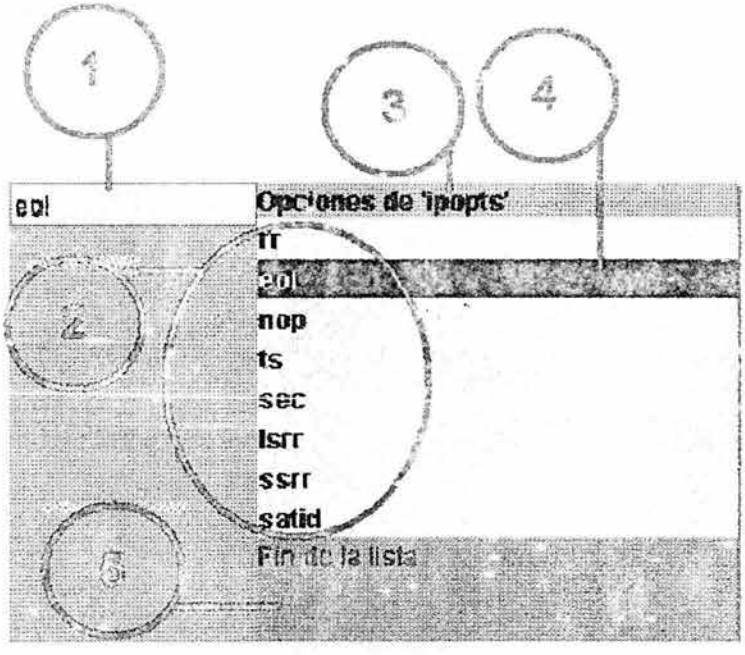

Figura 4. Campo para la introducción de alguna opción de la regla.

Aquí, para estas 4 imágenes, es importante hacer notar que cuando el usuario está recorriendo los campos donde se colocan cada una de las partes de la regla, en el momento en el que llega a un campo aparece la ventana que se muestra en las imágenes. Dicha ventana está formada por el título descriptivo, el cuadro de posibles opciones y el área del mensaje. Una vez que el usuario haya elegido, mediante las flechas hacia arriba y hacia abajo, la opción que desea, el mismo usuario, oprimiendo las flechas hacia la izquierda o hacia la derecha, podrá pasar al campo anterior o al siguiente respectivamente. De esta manera el usuario podrá navegar a través de los campos mediante las cuatro flechas de dirección.

Aunado a esta facilidad, el usuario también puede editar, mediante el tec
opción que desea, y con la tecla <<enter>> podrá pasar al siguiente campo.

Dicha ventana aparece cuando el usuario llega a un campo en donde se
y desaparece cuando salga de dicho campo. Aparece del lado derecho del campo,
parte inferior en caso de que no haya lugar para posicionarla del lado derecho.

Esas interfaces, recordemos, son solamente un prototipo, así que a la
implementarlas se puede plantear otra manera de presentación.

A continuación se presenta una imagen que nos indica la manera en
interfaz gráfica le indica al usuario que se ha equivocado al introducir la direcci
el campo.

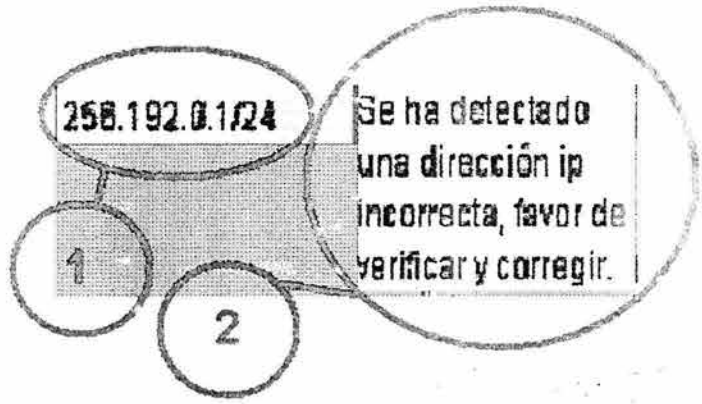

Figura 5. Indicación de error en la introducción de una dirección ip para la regla.

En esta figura podemos observar que se encuentra formada de dos partes.

1.Campo de introducción de ip. Es el campo de texto donde se introduci
correspondiente a la parte de la regla que se esté editando.
2.Mensaje de error. Este es un mensaje que aparece en una ventana
que la dirección ip introducida es errónea.

Vale la pena aclarar, en esta imagen, que la dirección ip que se presen
campo de texto correspondiente no es correcta ya que no puede empezar con el número
256. A partir de esta conjetura, la interfaz gráfica tiene que indicarle al usuario
equivocado en la introducción de un campo en la regla. Esta indicación
mediante la ventana de fondo amarillo que se presenta a su lado derecho.

Dicha ventana tiene la peculiaridad de que, debido a su fondo amari
letras azules, resulta ser llamativo para el usuario final. Esto logrará indicarle al
acerca de su error.

Igual que con las imágenes anteriores, esta es un prototipo de esta par
interfaz gráfica. La persona que implemente este sistema podrá proponer otra
presentar esta parte de la interfaz.

Otra manera de hacerlo llamativo es indicándole su error mediante el parpadeo del borde del campo de texto. Es decir, haciendo que el borde del campo de texto cambie de color, por ejemplo, de rojo a gris (o bien, en el caso de gris puede ser del color del fondo para que de una apariencia como que no tiene borde), de tal manera que de la apariencia de que pasa de tener un borde rojo a no tener borde. Esto repetido constantemente logrará la atención de los usuarios.

Apéndice B

Archivo principal de configuración del sistema Snort

Como ya se mencionó en el capítulo 4 (Sistema de Detección de Intrusos SNORT), el sistema Snort se configura a través de archivos.

El archivo principal tiene varias instrucciones que Snort interpreta de cierta manera, las instrucciones más importantes se detallan a continuación.

Incluye

Snort utiliza esta instrucción para mandar llamar el contenido de otros archivos formados por el usuario. De esta manera los archivos que contienen las reglas se mandan llamar con la instrucción 'include', la cuál tiene una sintaxis como la que sigue:

include: ruta_al_archivo_de_reglas.

Esta instrucción se puede colocar en dicho archivo tantas ocasiones como archivos se necesite agregar.

Comentarios

Snort también acepta comentarios dentro de los archivos de configuración. Snort toma como línea comentada, toda aquella línea que comienza con el símbolo '#'.

Variables

Las variables son constantes que se pueden declarar para su posterior uso dentro de los archivos de configuración. Esto se hace debido a que son constantes que se usan muy seguido dentro de la configuración de Snort. De tal manera que no hay que estar repitiendo el texto que contiene la variable.

La sintaxis para declarar una variable es la siguiente:

var: nombre valor

Reglas

Los archivos de reglas contienen todas y cada una de las reglas que Snort va a aplicar a los paquetes de datos circulantes en la red que se vayan a analizar.

El formato de las reglas se puede separar en varias partes:

- Cabecera de la regla. La cabecera de la regla contiene información acerca de quién, dónde y qué cosa de los paquetes va a hacer que dicha regla sea lanzada por Snort, así como la acción que se va a tomar cuando aparezca un paquete con la descripción de la regla.
- Opciones de la regla. Le indica a Snort que se va a revisar de cada paquete, de tal manera que si algún paquete coincide con lo que dice alguna regla, dicha regla es

lanzada y se ejecuta la acción que indica la regla.

Cada una de las partes mencionadas le indican a Snort lo necesario para analizar los paquetes de datos y ejecutar las acciones necesarias.

La descripción de las reglas se encuentra detallada en el Apéndice C.

Apéndice C

Componentes de las reglas de configuración de Snort

Como ya se mencionó en el capítulo 4, Snort trabaja mediante reglas de configuración. En este apéndice detallaremos cada uno de los componentes de dichas reglas de configuración.

Las reglas de configuración consta de dos partes: la cabecera de la regla, destinada a indicarle los datos de referencia de los paquetes de datos que pueden generar alguna alerta en el sistema o la red donde se encuentra instalado Snort; y las opciones de la regla, destinadas a detallar el contenido de los paquetes de datos que Snort tiene que detectar.

A continuación se detallan cada uno de los componentes de las dos partes de las reglas de Snort mencionadas.

Cabecera de la regla
Es la primera parte de las reglas y tiene la siguiente sintaxis:

acción protocolo dirección_ip:rango_puertos operador_dirección dirección_ip:rango_puertos

y la descripción de cada una de sus partes es la siguiente:

Acción tomada

La acción le indica a Snort de que manera va a actuar Snort en caso de que se presente un paquete que coincida con la regla y haga que ésta sea lanzada.

Hay 5 tipos de acciones que Snort acepta, las cuáles se describen a continuación:

alert. Snort genera un tipo de alerta. Aquí Snort utiliza el método de alerta seleccionado y posteriormente registra el paquete. La alerta es generada antes que el paquete sea registrado.

log. Se encarga de registrar el paquete que coincidió con la regla. Registra el paquete con el formato que se eligió en la línea de comandos al iniciar el funcionamiento de Snort.

pass. Permite pasar el paquete que coincide con esta regla. Snort, cuando se da cuenta que el paquete analizado cumple con lo que la regla en cuestión dice lo deja pasar y permite que continúe con su camino hacia su destino.

activate. Esta acción le dice a Snort que alerte al administrador del sistema y posteriormente activa otra regla de tipo dinámica. La alerta que se genera primero se envía con el formato y hacia el conducto que se eligieron en la línea de comandos. Luego activa otra regla, para que esta otra ejecute la acción que indica.

dynamic. Este tipo de reglas permanecen activas, pero en estado de espera, hasta que alguna regla de tipo 'activate' las active. Una ves que son activadas actúan

como una regla de tipo 'log'. Una ves que realiza su tarea vuelve al estado de espera.

Protocolo

El protocolo le indica a Snort el tipo de protocolo al que pertenece el paquete, es decir, el protocolo mediante el cuál el paquete fue enviado por la computadora origen.

Snort acepta el análisis de 4 protocolos: tcp, udp, icmp e ip

En un futuro se espera que los siguientes protocolos sean aceptados por Snort: arp, igrp, grep, ospf, rip e ipx.

El paquete de datos que circula por la red trae indicado el protocolo en una parte de su cabecera de datos, por lo que Snort lo que realíza es leer dicha parte de la cabecera del paquete de datos y, a partir de allí, identifica si hay que analizar dicho paquete.

Dirección IP

La dirección ip indica la dirección de la computadora que origina el paquete, así como la dirección de la computadora a la que va dirigido el mismo. La primera se coloca antes del operador de dirección y la segunda se coloca después del mismo.

Dicha dirección viene indicada en la cabecera del paquete de datos. A partir de aquí Snort revisa si concuerda con el indicado en la regla.

La manera en que se indican dichas direcciones es con el formato CIDR, de otra manera Snort no la va a poder entender.

En este rubro también se puede utilizar la palabra clave 'any', la cuál indica que se cotejarán con la regla los paquetes que cumplan con cualquier dirección ip, es decir, todos los paquetes.

Existen otros operadores que se pueden usar en esta sección. El operador '!' le indicará al Snort que las direcciones indicadas no serán revisadas, es decir es un operador de negación.

Número de puerto

Es el rango de puertos en el que puede estar el paquete analizado.

El puerto de la computadora de origen se coloca antes del operador de dirección, y el puerto de la computadora destino se coloca después del mismo operador.

Cuando un paquete de datos es generado y enviado a través de una red, incluyendo internet, es enviado desde una puerto en la computadora origen (es el puerto de origen) y va dirigido hacia un puerto en específico en la dirección destino (es el puerto destino), dicho puerto viene indicado en la cabecera del paquete en cuestión.

Si los puertos de origen y destino están dentro del rango indicado en la regla quiere decir que el paquete puede seguirse analizando con la regla en cuestión.

El rango de puertos se expresa con la siguiente sintaxis:

puerto_inicio:puerto_final

donde puerto_incio es el número de puerto en donde inicia el rango, así como puerto_final es el número de puerto donde termina el rango de puertos. Todos los puertos que estén dentro de dicho rango son los que Snort va a tomar en cuenta cuando revise las cabeceras de los paquetes de datos de la red en donde se instalará.

En este rubro también se puede utilizar la palabra clave 'any', la cuál indica que se cotejarán con la regla los paquetes de cualquier puerto, es decir, todos los paquetes.

Existen otros operadores que se pueden usar en esta sección. El operador '!' le indicará al Snort que el rango de puertos que le sigue a este operador será el rango de puertos que no serán revisados, es decir es un operador de negación.

Operador de dirección

El operador de dirección indica el flujo[1] en el que va el paquete. Este operador se coloca entre la dirección ip (incluyendo el puerto) de origen y la dirección ip (incluyendo el puerto) destino. Este operador se indica con una flecha que va en dirección de izquierda a derecha (->), o bien, una flecha que indica que va en ambas direcciones (<>).

De esta manera uno puede construir la primera parte de las reglas que harán que Snort detecte los paquetes.

Opciones de la regla.

Esta sección de Snort se considera como el corazón del mismo, ya que es la parte de las reglas que le indican las características con las cuáles los paquetes deben coincidir para que dicha regla sea lanzada y se pueda ejecutar la acción que es indicada por la misma.

Esta sección se encuentra encerrada entre paréntesis, y dentro se encuentran las opciones de la regla. Se coloca justo después de la cabecera de la regla.

[1] Sentido en que se mueve el paquete de datos.

Cada opción se encuentra separada una de otra por medio de un punto y coma (;), también viene acompañada de un valor, en caso de que se necesite, y el valor viene separado del nombre de la opción por el símbolo (:).

Un ejemplo de las opciones de reglas es el siguiente:

(fragbits: R+; msg: "Rerserved bit set!";)

Las opciones que Snort acepta son 41. Se describen a continuación.

msg.
Imprime un mensaje en la alerta generada por Snort, así como en el registro del paquete.
logto.
Registra el paquete en un archivo especificado por el usuario en lugar del archivo indicado en la salida estándar.
ttl.
Los paquetes de datos contienen en su cabecera una sección que se llama 'campo[2] ttl', esta opción le indica a Snort que debe de revisar su contenido y cotejarlo con el valor indicado.
tos.
Los paquetes de datos contienen en su cabecera una sección que se llama 'campo tos', esta opción le indica a Snort que debe de revisar su contenido y cotejarlo con el valor indicado.
id.
Los paquetes de datos contienen en su cabecera una sección que se llama 'campo id', esta opción le indica a Snort que debe de revisar su contenido y cotejarlo con el valor indicado.
ipoption.
Esta opción le indica a Snort que debe de observar el campo de las opciones de IP de la cabecera del paquete de datos y verificar si concuerdan con los especificados por el administrador de Snort en las opciones de la regla.
fragbits.
Coteja los bits de fragmentación que se encuentran en la cabecera de el paquete de datos con los que el administrador de Snort indicó en las opciones de dicha regla.

[2] La cabecera de los paquetes IP se dividen en varias secciones llamados campos. Cada sección contiene datos descriptivos de alguna característica del paquete IP. Estos los usan los programas para identificar las características de los paquetes que viajan por internet.

dsize.
Checa que el valor del tamaño de los datos que contiene el paquete concuerden con los especificados por el administrador del sistema Snort en las opciones de dicha regla. Los datos que contiene el paquete son todos los datos que vayan en el paquete menos los que pertenecen a la cabecera del mismo.
flags.
Dentro de la cabecera del paquete de datos existe una sección que contiene banderas llamadas 'banderas de TCP', las cuáles indican estados del paquete respecto al protocolo TCP. Con esta opción, dichas banderas son cotejadas con las que el administrador del sistema Snort indicó.
seq.
Dentro de la cabecera del paquete de datos existe una sección que contiene banderas llamadas 'números de secuencia de TCP[3]', las cuáles indican el orden que tienen que llevar los paquetes enviados. Con esta opción, los valores son cotejados con las que el administrador del sistema Snort indicó en la regla.
ack.
Dentro de la cabecera del paquete de datos existe una sección que contiene banderas llamadas 'campo acknowledgement de TCP'. Con esta opción le indicamos a Snort que debe de cotejar dichos valores con los indicados en la regla.
itype.
En los paquetes que sean del protocolo ICMP[4] existe un campo llamado 'type'. Esta opción se encarga de cotejar el valor de dicho campo con el valor dado en la regla.
icode.
Dentro de la cabecera de los paquetes que sean del protocolo ICMP existe un campo llamado 'code'. Esta opción se encarga de cotejar el valor de dicho campo con el valor dado en la regla.
icmp_id.
Dentro de la cabecera de los paquetes que sean del protocolo ICMP existe un campo llamado 'id'. Esta opción se encarga de cotejar el valor de dicho campo con el valor dado en la regla.
icmp_seq.
Esta opción coteja el valor dado con el valor del campo, que se encuentra en la cabecera del paquete, llamado' seq en los paquetes de protocolo ICMP. Dicho campo de la cabecera cumple las mismas funciones que el campo seq de los paquetes del protocolo TCP.

[3] Dicha secuencia de números se utiliza cuando los datos enviados por internet son muy grande y se tienen que enviar por medio de varios paquetes, esta secuencia indica el orden que los paquetes tienen que seguir para volver a formar los datos completos.
[4] Protocolo usado en internet para la transmisión de datos.

content.
El valor que se le asignará a esta opción se cotejará con el contenido de datos del paquete. Esto es, Snort toma el contenido de datos del paquete y revisa si en el se encuentra la cadena de datos que esta opción indica. Básicamente revisa si el valor de la opción se encuentra dentro del paquete de datos.
content-list.
Realiza lo mismo que la opción anterior, con la diferencia de que en esta opción se le puede dar como valor varias cadenas de datos para que Snort las coteje con los datos del paquete.
offset.
Cuando Snort usa las dos opciones anteriores, las cuáles nos permiten buscar una cadena de datos dentro de los datos del paquete, uno le puede indicar desde donde empezar a buscar mediante esta opción. Es decir, este es el número de bytes al principio de los datos del paquete donde Snort no va a buscar dicha concordancia con la cadena de datos escrita en las opciones 'content' o 'content-list'. De esta manera uno le indica a Snort que no busque en la primera parte de los datos del paquete.
depth.
Cuando Snort usa las opciones 'content' y 'content-list', donde tiene que buscar si los valores dados para esas dos opciones se encuentran en los datos del paquete, uno le puede indicar, mediante esta opción, el número de bytes que revisará para verificar si existe las cadenas de datos dadas dentro de dicho número de bytes. El número de bytes indicado en esta opción comienza desde el principio de los datos del paquete, al menos que la opción 'offset' esté activada e indique que tiene que empezar a buscar desde otra posición, en cuyo caso los bytes se contarán desde dicha posición.
nocase.
Cuando Snort realiza una búsqueda, donde intervienen las 4 opciones anteriores, dicha búsqueda la realiza tomando en cuenta las mayúsculas y las minúsculas de la cadena dada, es decir, la cadena de datos tiene que ser igual en los datos del paquete. Con esta opción uno le puede indicar a Snort que al buscar no se fije en mayúsculas o minúsculas, es decir, que baste solamente que coincidan en las letras contenidas en la cadena de datos, no importando si algunas son mayúsculas o minúsculas, de las opciones 'content' o 'content-list'.
session.
Cada paquete de datos, en su cabecera contienen un campo que indica la sesión del paquete en el sistema operativo. El valor de dicho campo es cotejado con el valor especificado en esta opción.
rpc.
Observa cuáles servicios de tipo RPC[5] contiene el paquete para las llamadas de procedimiento o de aplicación especificadas.

[5] Remote Procedure Calling, en sus siglas en inglés. Es un protocolo de comunicación entre computadoras en internet.

resp.

Permite a Snort cerrar las conexiones que se consideren ofensivas.

react.

Permite activar una respuesta en contra de las páginas web que uno desea. La respuesta puede ser el no permitir visitarla o no permitir que la página indicada envíe datos.

reference.

Permite a Snort decirle acerca de referencias a sistemas de identificación de ataques externos.

sid.

Esta opción le permite a Snort identificar a las reglas escritas con un número único de identificación. Esto es muy útil ya que Snort, en el momento en que genera una salida, imprime dicho número, y cuando uno quiere ver que reglas han generado las salidas pues dicho número nos lo indicará.

rev.

Es utilizada por Snort para realizar identificaciones de revisiones de reglas.

classtype.

Esta opción permite categorizar a las reglas, es decir, agruparlas por el tipo de ataque del que se trate. Esto es muy útil porque se le puede decir a Snort que le de prioridad a las reglas que sean de cierta clase. Con esto Snort puede ejecutar primero dichas reglas y después las otras.

priority.

Esta opción permite asignarle el nivel de prioridad con que queremos que Snort la trate. Es decir, si uno le coloca un nivel de prioridad más alto que las demás, Snort va a ejecutar primero esta regla. Y de manera contraria, si uno le coloca una prioridad baja, Snort la ejecutará hasta el último.

uricontent.

Permite buscar patrones de contenidos dentro de la porción URI[6] de el paquete de datos. Nótese que solamente buscará en la porción URI del paquete. Esta solamente funciona junto con el codificador de HTTP[7] especificado por el administrador del sistema Snort, el cuál se explica más adelante.

tag.

Le indica a Snort que en el momento en que una regla sea lanzada, en vez de solamente guardar el paquete, que guarde más que eso. Cuando un paquete indica que una regla es lanzada se genera un tráfico extra referente a la computadora

[6] Uniform Resource Identifier en sus siglas en inglés. Es una manera compacta de representar, mediante una cadena de caracteres, un recurso físico o abstracto.

[7] Protocolo utilizado en internet para realizar peticiones a otras computadoras.

envió el paquete, dicho tráfico es el que también se registra. Esto es muy útil cuando el administrador del sistema Snort quiere analizar los movimientos habidos después de que la regla fue lanzada.

ip_proto.

Permite verificar el tipo de protocolo que el paquete tiene. Esto resulta muy cuando uno sabe que cierto ataque informático se realiza con algún protocolo específico. De esta manera uno puede hacer que Snort, antes que nada, verifique el protocolo del paquete de datos, y, en caso de que no sea el deseado, pues no lo siga revisando y se pasa a la siguiente regla.

sameip.

Uno de los casos más conocidos de ataques es el que provoca el DOS[8], el cual en pocas palabras, el paquete que llega a la computadora, en su cabecera, contiene la misma dirección ip tanto en la dirección ip destino como en la dirección ip origen, esto provoca un error en la computadora. Con esta opción Snort verifica si los paquetes que llegan a la computadora tienen esa peculiaridad, y en caso de que sea así, lanza la regla que se esté verificando. Esta opción es muy útil para detener ataques tan comunes como el que se explico.

stateless.

Esto le indica a Snort que debe de validar el paquete independientemente del estado del flujo.

regex.

Aunque este módulo está todavía en vías de desarrollo, lo que permite es que Snort, mediante una expresión regular, busque diversos contenidos dentro de los datos útiles[9] del paquete de datos.

---

[8] Denial Of Service en sus siglas en inglés. Dicho ataque es muy común dentro de internet, aunque actualidad muchas de las empresas que están propensas a dicho ataque ya los han controlado. Este es muy sencillo, consiste en lo siguiente: la computadora origen genera un paquete de datos que en una petición de inicio de sesión, en donde dicho paquete le coloca la misma dirección en dirección destino y en la dirección origen y lo envía a la computadora correspondiente. Dicha dirección colocada es la dirección ip de la computadora destino. Una ves que la computadora destino recibe el paquete, al darse cuenta que es una petición de comienzo de sesión, envía una respuesta de aceptación a la dirección ip indicada en el campo de dirección origen de la cabecera del paquete de datos, y se queda esperando la respuesta de la otra computadora. Dado que la dirección origen es la misma dirección de la computadora destino, ésta última envía una respuesta a sí misma. En dicha respuesta, en la cabecera del paquete imprime su dirección ip en los campos dirección ip destino (dirección a donde envía la respuesta) y dirección ip origen (dirección desde donde se origina el paquete de datos). Dado que la dirección destino su misma dirección, dicho paquete le llega en el instante en que la envió, lo cuál provoca que lo interprete como una petición de inicio de sesión, por lo que vuelve a generar un paquete de respuesta de la misma forma. Este proceso se repite constantemente, y, dado que en cada petición la computadora origen se queda esperando la respuesta de la computadora origen, y eso implica que la computadora destino reserve un pedazo de memoria para la pila de peticiones, después de un rato se encuentra esperando varias, o en ocasiones muchas, respuestas de la misma computadora. Y, dado que la memoria que se utiliza para almacenar la pila de peticiones es limitada llega un momento en que se acaba y el servidor no tener más memoria interrumpe el servicio que proporcionaba por el puerto en el que se estaban realizando las transacciones.

[9] Parte del paquete de datos que no pertenecen a la cabecera del mismo.

byte_test.
Dentro de la cabecera del paquete existe un campo llamado 'byte'. Con esta opción verifica si el valor dado por el administrador del sistema Snort coincide con el valor de dicho campo.
distance.
Permite a Snort realizar una búsqueda dentro de los datos del paquete en el número de bytes indicados mediante esta opción.
within.
Funciona de manera similar a la opción explicada anteriormente de nombre 'distance'.
byte_jump.
Funciona como la opción 'offset'. Le indica a Snort cuántos bytes debe dejar pasar antes de empezar a realizar la búsqueda dentro de los datos del paquete.
flow.
Le indica a Snort que dicha regla se aplicará solamente cuando el flujo del paquete sea en cierta dirección. Las direcciones del flujo del paquete que Snort acepta en esta opción son cuando el paquete va hacia el cliente, cuando el paquete va hacia el servidor, cuando el paquete viene del cliente, cuando el paquete viene del servidor, entre otros. Esto permite al administrador del sistema Snort limitar los paquetes revisados dependiendo de la dirección que lleven.
rawbytes.
Permite que Snort , cuando observe paquetes de datos codificados para la aplicación telnet, procese los datos de manera desnormalizada.

Estas son todas las posibles opciones que la regla de Snort tiene, para su formación, que le permiten hacerlo muy flexible en cuanto a su funcionamiento.

La sintaxis que debe seguir la parte de las opciones de la regla es la siguiente:

(opcion:valor[;opcion:valor]*)

Es importante hacer notar algunos aspectos: las opciones se colocan entre paréntesis; la separación entre cada opción es mediante el 'punto y coma'; y por último la separación que hay entre el nombre de la opción y su valor se da mediante un sencillo 'dos puntos'.

Esta sección, la de opciones, se coloca inmediatamente después de la sección de la cabecera de la regla.

La sintaxis completa que deben seguir las reglas en Snort es la siguiente:

cabecera_de_regla (opciones_de_regla)

Si alguna de ambas partes se encuentra mal escrita o tiene algo incorrecto, Snort detendrá su funcionamiento y saldrá de la ejecución, y desplegará un mensaje avisando cual es la regla que es incorrecta.

Por último, veamos todo lo anterior reunido a través de un ejemplo práctico de una regla bien formada que se podría usar dentro de la configuración del sistema Snort dentro de sus archivos.

alert tcp $HOME_NET 21 -> $EXTERNAL_NET any (msg:"FTP Bad login"; content:"530 Login "; nocase; flow:to_server,established; classtype:bad-unknown; sid:491; rev:4;)

En esta regla se puede observar que va a generar una alerta (**alert**) cuando Snort se tope con un paquete que tenga el protocolo TCP (**tcp**) que vaya desde la red indicada por la variable **$HOME_NET,** y que salga del puerto **21,** hasta la red indicada por la variable **$EXTERNAL_NET**, y que vaya hacia cualquier puerto, y que cumpla con las opciones que se presentan dentro del paréntesis.

La regla debe de estar en un solo renglón para que Snort la pueda leer de manera correcta, en caso contrario generará un error al leerla. En caso de que el administrador de Snort quiera tenerla en varios renglones tiene que colocar el símbolo (/) al final del renglón para que Snort pueda saber que la regla está formada en varios renglones.

Con lo anterior uno puede generar cualquier cantidad de reglas de acuerdo a las necesidades de protección de la red. Esto es, Snort nos permite tener el número de reglas necesarias, pero bien formadas, para la protección completa de la red en que se encuentra instalado. Esto hace a Snort más flexible.

Apéndice D

Componentes de GSnort Servidor

Ya en el capítulo 5 se mencionaron los componentes de GSnort Servidor, en este apéndice se busca detallar el funcionamiento de cada uno de dichos componentes.

Para retomar un poco la estructura de GSnort Servidor se presenta la configuración de los componentes dentro de este mediante la siguiente figura (presentada en el capítulo 5):

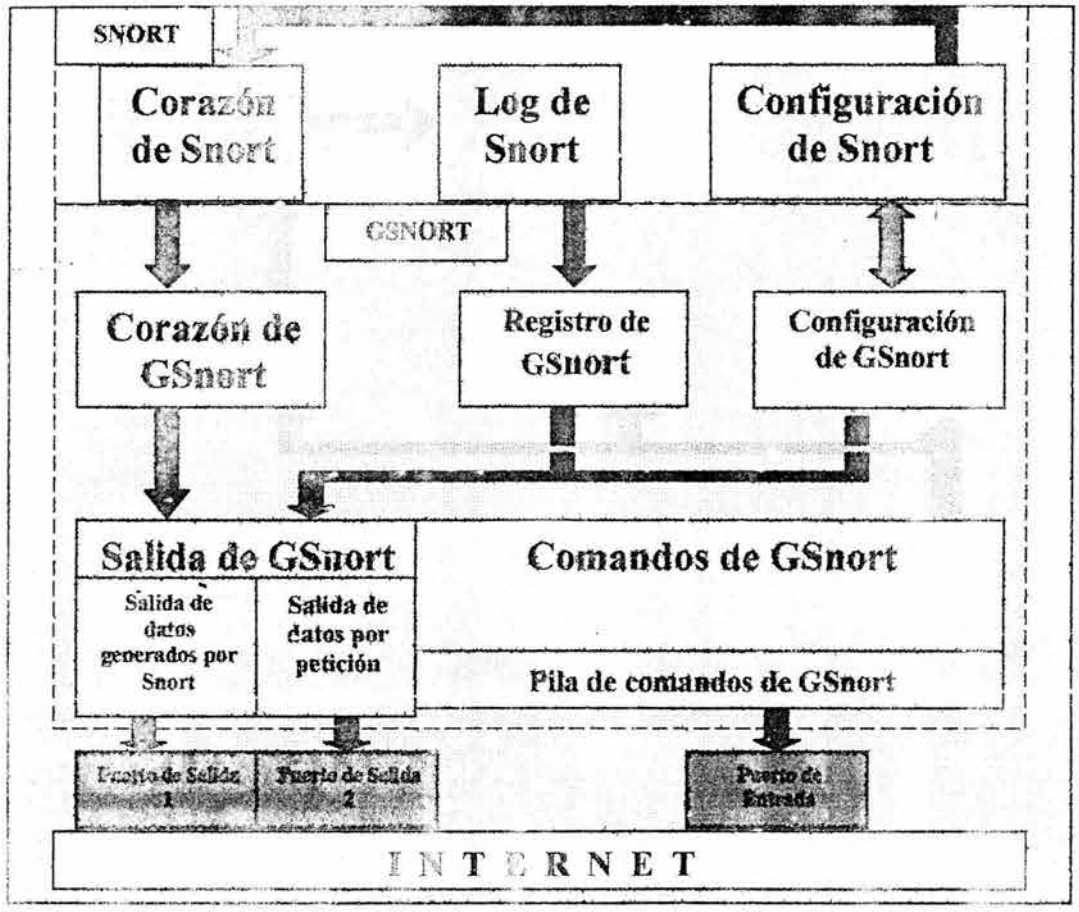

Figura D-1. Estructura de GSnort Servidor

Y a continuación el detalle de cada uno de los componentes.

Corazón de Snort

Es la ejecución propia del sistema Snort, encargada de llevar a cabo el análisis de los paquetes y ejecución de acciones de acuerdo a las reglas estipuladas en los archivos de configuración. Es el corazón[1] del sistema, el módulo que realiza todas las tareas necesarias para proteger a la computadora o a la red de computadoras.

Toma los datos de configuración del módulo llamado 'Configuración de Snort'.

Log de Snort

Conjunto de archivos donde Snort registra los movimientos, análisis y acciones que lleva a cabo a raíz de las instrucciones dadas por los archivos de configuración.

Esta parte de Snort aumenta conforme se generen nuevos reportes de actividades sospechosas. Y aumenta aún con mayor rapidez si el tráfico en la red es denso, ya que aumenta las posibilidades de actividades sospechosas.

Configuración de Snort

Conjunto de archivos que Snort utiliza para su configuración. Aquí se le indica de que manera va a analizar a los paquetes y acciones de acuerdo al contenido de dichos paquetes. Contienen las reglas de configuración, variables, plugins[2], instrucciones de preprocesador y todas aquellas instrucciones que Snort necesita para que su funcionamiento vaya acorde a nuestras necesidades.

Este conjunto de archivos es hecho por el administrador del sistema Snort y, aunque la instalación de Snort tiene ya muchos predeterminados, uno los puede configurar de acuerdo a nuestra conveniencia.

Corazón de GSnort

Encargada de manipular el programa principal del sistema Snort.

Funciones: arrancar el sistema Snort, detenerlo, tomar los datos que Snort genera para transmitirlo a algún cliente.

Recibe instrucciones de parte del módulo llamado 'Comandos de GSnort' acerca de lo que tiene que ejecutar

Registra cada una de las operaciones dadas por los comandos que el cliente envía al servidor y que realiza GSnort. Son guardadas en un archivo con un formato, el cual es definido en los archivos de configuración de GSnort.

[1] En el mundo de la computación se le conoce de esta manera a la parte medular de el sistema.
[2] Pequeños módulos que se le pueden agregar a Snort para incrementar su funcionalidad.

Entre las instrucciones que 'GSnort Command' le puede indicar a 'GSnort Core' están las siguientes:

- Iniciar Snort

Permite arrancar el funcionamiento de Snort. Solamente consiste en eso.
Le envía al sistema Snort una señal para que arranque su funcionamiento, abriendo, así mismo, un flujo de datos a través del cual el sistema Snort enviará sus resultados a un 'pipe[3]' de datos. A través de dicho 'pipe' GSnort recibirá los datos que envíe Snort.
El siguiente diagrama expresa de manera gráfica el funcionamiento de esta instrucción.

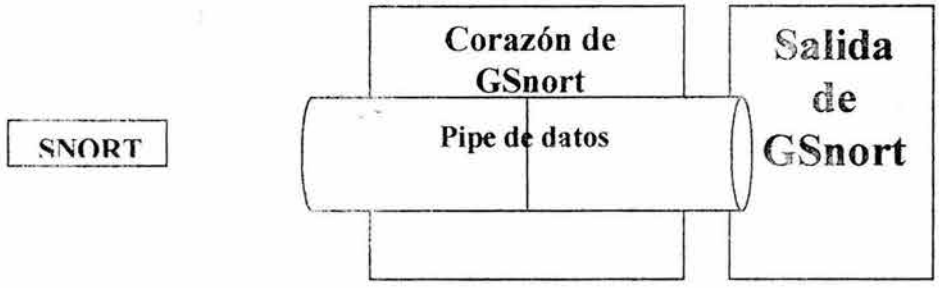

Figura D-2. Modo de funcionamiento de la función 'Iniciar Snort'

- Parar funcionamiento del sistema Snort

Indica al Corazón de GSnort que detenga el funcionamiento del sistema Snort.
Cuando se ejecuta este comando Snort interrumpe el flujo de datos. Con esto se deja de transmitir datos al cliente.
Cuando esta operación es ejecutada el estado del diagrama anterior queda de la siguiente manera:

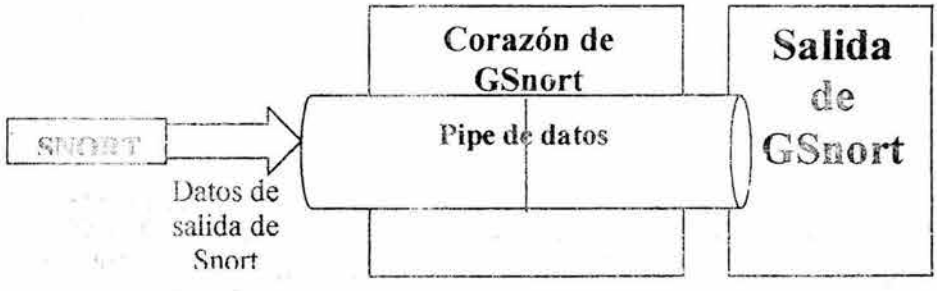

Figura D-3. Modo de funcionamiento de la función 'Parar Snort'

[3] Se puede interpretar como un tubo por donde circulan los datos de salida de un programa. En el diagrama es el tubo que se observa con el nombre de 'flujo de datos'.

Con esto, el sistema Snort dejara de funcionar, por lo que la red estará expuesta a ataques informáticos, ya que Snort no estará analizando ningún paquete que entre a la red. Debido a esto se tiene que tener mucho cuidado cuando se ejecuta dicha operación.

- Reiniciar el funcionamiento de Snort
Indica al Corazón de GSnort que detenga y arranque el sistema Snort.
En ese momento el sistema Snort puede estar en varios estados, los cuales definen el comportamiento del Corazón de GSnort. Para cualquiera de los estados en que se encuentre el sistema Snort, el Corazón de GSnort tendrá que realizar algunas verificaciones, las cuales consisten en ver si el sistema Snort se encuentra funcionando o si se encuentra apagado.
Estado 1. Sistema Snort apagado. El Corazón de GSnort le envía la señal correspondiente al sistema Snort para que arranque su funcionamiento.
Estado 2. Sistema Snort funcionando. Transmite dos señales, la primera para detener su funcionamiento, y la segunda para arrancarlo de nuevo.
Las señales se envían una tras otra para que no exista mucho tiempo sin que el sistema Snort esté sin funcionar.

- Transmitir Datos al Cliente
Indica a GSnort que debe de parar el flujo de datos que provienen de Snort.
Esto se puede ver más claramente en el diagrama siguiente:

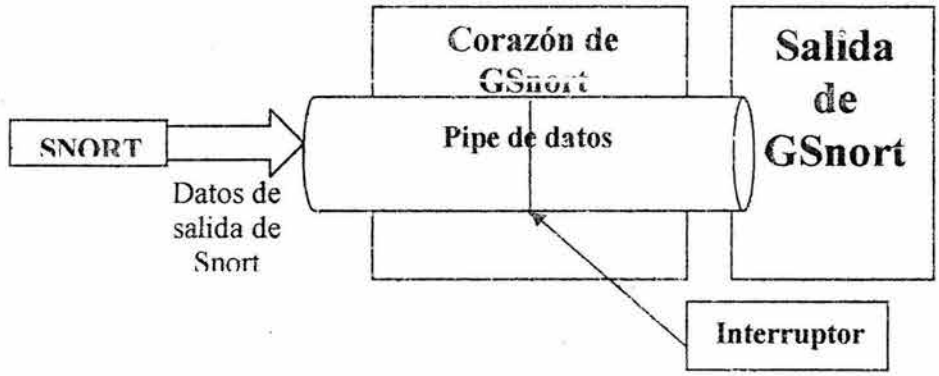

Figura D-4. Modo de funcionamiento de la función 'Reiniciar Snort'

Cuando el interruptor esta desactivado, el Corazón de GSnort deja de leer los datos que envía Snort, sin detener su funcionamiento. Es decir, Snort sigue enviando datos de salida, pero GSnort no los lee, por lo que el módulo de Salida de GSnort no recibirá datos y no se enviará nada de datos al cliente.
Por el contrario, si el interruptor se encuentra activado, el Corazón de GSnort leerá de manera constante los datos que envía Snort y los reenviará al módulo de Salida de GSnort para que este último los envíe a GSnort Cliente.

- Parar Transmisión de datos al Cliente
Indica al Corazón de GSnort que deje de leer el flujo de datos que envía el sistema Snort, esto interrumpirá el flujo de datos al módulo de Salida de GSnort.

Cuando se ejecuta esta instrucción por el Corazón de GSnort se desactiva el interruptor intermedio. Pero el funcionamiento del sistema Snort sigue normal.

Este módulo registra cada una de las operaciones realizadas en un archivo que se le indica en la configuración del sistema GSnort.

Registro de GSnort

Lee los archivos de registro del sistema Snort, les da formato para que el cliente los pueda leer y los envía al cliente en caso de que este último los pida.

Su funcionamiento es muy sencillo, las instrucciones que el Registro de GSnort puede recibir son las siguientes:

- Leer archivos de registro
Solamente lee los archivos de registro de Snort y los guarda en memoria.
Ya que los archivos de registro pueden ser muy numerosos o muy grandes en espacio en disco y pueden causar que, cuando los lea y los tenga en memoria, ocupen mucha memoria, esta instrucción tiene banderas de restricción en donde se le puede indicar cuáles archivos debe leer y cuáles no debe de leer.
Con esto uno puede restringir los archivos que lea de acuerdo a la ip, al puerto, aplicación u otra característica que haya dado paso a la generación del mismo.
Dichas banderas de restricción son expresiones regulares que definen los patrones a seguir en la elección de los archivo, y datos en el archivo elegido, que se levantarán[4] a memoria. Dichas expresiones regulares se brindan para ip que generan los archivos, puertos hacia donde llegan los paquetes de datos, protocolo, datos del mismo paquete, así como del tipo de acción que provocó.
En caso de que no se le indique alguna expresión regular para restringir los datos que se tienen que leer, los comandos del Registro de GSnort tienen valores predeterminados para leer dichos datos.

- Dar formato[5] a archivos de registro
Indica al Registro de GSnort que los archivos leídos con la instrucción anterior se les asigne el formato necesario para que GSnort Cliente los pueda leer con facilidad y los pueda desplegar al administrador del sistema GSnort.
En caso de que no haya archivos levantados en memoria, no se da formato a ningún archivo.
En caso de que los archivos levantados a memoria no se les asigne formato, los archivos se enviarán sin formato y se podrán leer de manera normal, ya que enviará el archivo entero, tal cual como se encuentra en el disco duro.

[4] Poner los datos en memoria ram.
[5] Consiste en colocarlos de una manera especial para que el cliente los pueda leer.

- Enviar archivos a cliente
Indica al Registro de GSnort que envíe los datos al cliente.
Solamente envía los datos que se tienen en memoria, ya sea con formato o sin él, a través del puerto de salida correspondiente.

- Borrar los archivos que tiene en memoria.
Indicarle al Registro de GSnort borrar todos los archivos que tiene en memoria. Se libera la memoria utilizada para almacenar los archivos pedidos anteriormente.

Una vez ejecutado esta instrucción ya no se puede recuperar los archivos que se tenían en memoria. Para eso se tienen que volver a leer y subir a memoria.

Cada una de las operaciones que se realizan en este módulo se registran en el archivo indicado en la configuración de GSnort.

Configuración de GSnort

Encargado de interactuar con los archivos de configuración del sistema Snort.

Ya que el sistema Snort contiene un gran número de archivos, así como una variedad de instrucciones y reglas para su configuración, es necesario tenerlos ordenados para que puedan ser accedidos con rapidez y prontitud por el cliente.

Para cada una de las partes que Snort utiliza para su configuración (variables, reglas, etc), GSnort tiene un contenedor[6] que se encarga de manejarla. Con esta manera de trabajar, GSnort tiene el control total de todos los archivos de configuración, de manera ordenada, que utiliza Snort, y por ende los tiene accesibles.

Para lograr esto, GSnort comienza por leer el archivo principal de configuración, el cual se le da a Snort cuando se arranca su funcionamiento. Cuando lo abre empieza a leer instrucción por instrucción y va guardando cada instrucción en su contenedor correspondiente. En el momento en el que se encuentre con una instrucción de tipo 'include', agrega dicha instrucción al contenedor correspondiente y continúa, antes de ir a la siguiente instrucción, con la lectura del archivo que se incluye. Cuando termina de leer el archivo correspondiente se regresa a la instrucción en que se quedo en el archivo anterior y prosigue con la lectura. Esta operación la realiza hasta que termine de leer el archivo principal de configuración, de tal manera que cuando llegue ese momento GSnort ya tendrá en sus contenedores todas las partes de configuración necesarias para su manipulación.

Para lograr esto, GSnort almacena cada una de las instrucciones individuales en un tipo de clase, correspondiente a cada instrucción.

[6] Puede verse como una clase que guarda las características de la parte en cuestión para su posterior manipulación. Por ejemplo, para manejar cada una de las reglas GSnort tiene una clase que se encarga de manejar dichas reglas, las cuáles son guardadas en otro contenedor encargado de guardar un conjunto de reglas, el cuál este último se puede observar como si fuera un archivo de configuración que contiene únicamente reglas de configuración de Snort.

De esta manera se tienen clases para varias partes de la configuración de Snort:

- Variable
Guarda una sola variable de la configuración de Snort.

- Include
Guarda una instrucción de tipo 'include' de la configuración de Snort.

- Config
Guarda una instrucción de tipo 'config' de la configuración de Snort.

- Reglas
Almacenar una sola regla de la configuración de Snort. Consta de dos partes, la cabecera y las opciones de la regla:

  - Cabecera
  Almacena únicamente la cabecera de la regla.
  - Opciones
  Almacena únicamente las opciones de la regla leída.

- Preprocessor
Almacena las instrucciones de tipo 'preprocessor' de la configuración de Snort.

- Output Modules
Almacena una instrucción de tipo 'output module' de la configuración de Snort.

- Plugins
Almacena una instrucción de tipo 'plugin' de la configuración de Snort.

En el interior de cada una de los contenedores mencionados están los campos necesarios para almacenar cada una de las partes de dichas instrucciones, así como métodos para su manipulación.

Una capa más arriba en la estructura del módulo de Configuración de GSnort se encuentra los contenedores de cada una de las instrucciones que Snort utiliza para su configuración. Es decir, cuenta con un contenedor para cada tipo de instrucción que tiene Snort dentro de su configuración. De tal manera que todas las instrucciones de tipo 'variable' (almacenadas cada una en una clase) se guardan en un contenedor (el cual es otra clase) llamado 'Variables', y así con cada tipo de instrucción.

GSnort también implementa un contenedor de archivos de configuración, el cual se puede ver como un manejador de estos. Este contenedor, al momento de leer los archivos de configuración coloca dentro de si un contenedor que almacena cada una de las líneas que tiene cada archivo. Este contenedor tiene en su interior métodos para la manipulación de cada una de las partes del archivo.

Por último, al momento de leer todos los archivos de configuración de Snort los coloca en memoria con la estructura ya vista. Esto se hace cuando se le pide que lea los archivos del servidor, pero cuando el cliente los modifica en su computadora y los envía de regreso, GSnort no borra lo que ya tiene, sino que coloca en otro apartado de

[7] Contenedor que maneja todos los contenedores de los datos con formato de GSnort Conf.
[8] Esto agiliza los trámites ya que enviar datos al servidor constantemente implica tiempo en que se envían y se regresa una respuesta.

la memoria todo lo que recibe en el formato ya explicado.

Esto quiere decir que GSnort utiliza dos lugares en memoria para almacenar los datos del servidor y los datos que envía el cliente. Al primero se les llamarán datos de primer plano, y al segundo se les llamarán datos de segundo plano.

Por lo anterior, se puede concluir diciendo que los datos que vengan del cliente se guardarán en el compartimiento de segundo plano de la memoria.

Otro plano de memoria es el que se utiliza para colocar archivos leídos que están sin formato. A este plano se le llamará plano cero.

Las instrucciones que puede realizar este módulo son las siguientes:

- Leer archivos y colocarlos en plano cero
Lee los archivos y los guarda tal cual están en disco duro, sin ninguna especie de formato. En cuanto los lee, los coloca en el plano cero para cuando se necesiten usar.

- Enviar datos de plano cero
Envía al cliente los archivos que se encuentren en el plano cero. Y los envía a través del puerto de salida determinado.

- Enviar datos de primer plano
Envía al cliente los datos que se encuentran en el primer plano de la memoria. Cuando envía estos datos del primer plano de la memoria, todos los contenedores que maneja GSnort Conf son colocados en un meta-contenedor[7] y son enviados a través del puerto de salida correspondiente, de tal manera que el cliente los pueda recibir todos en un mismo contenedor y a partir de allí poder manejarlos.
Para que haya datos en esta parte de la memoria, hace falta que se lean los archivos, se coloquen en el plano cero de la memoria, se lean los archivos de este último plano y se les de formato para que se guarden en esta parte de la memoria.

- Borrar datos de primer plano
Elimina los datos que se encuentran en el primer plano de la memoria.Libera memoria para ser utilizada por otros módulos de GSnort. Los datos que se encuentran en este plano de la memoria son borrados y no se podrán recuperar al menos que se vuelvan a leer y dar formato.

- Borrar datos de segundo plano
Elimine los datos que se encuentran en el segundo plano de la memoria.
Libera memoria para ser utilizada por otros módulos de GSnort, pero los datos perdidos solamente se recuperan si el cliente los vuelve a enviar.

- Recibir datos del cliente
Cuando el cliente pide los datos de los archivos de configuración a GSnort Servidor, este último se los proporciona (después de una serie de operaciones previas). Una ves que el cliente los tiene los puede modificar sin enviar datos al servidor[8], y, una ves modificados y estando seguro de que no se le va a realizar

otra modificación, los envía de regreso con todo y cambios hechos.
Dichos datos que envía el cliente, son enviados mediante esta instrucción, en donde GSnort los recibe y los coloca en el segundo plano de la memoria para tenerlos allí mientras GSnort los usa.

- Actualizar datos de configuración
Toma los datos que se encuentran en el segundo plano de la memoria y los guarda en disco duro. Los archivos de configuración de Snort se actualizarán de acuerdo a los datos contenidos en el segundo plano de la memoria.
Todos y cada uno de los archivos contenidos en la configuración del sistema Snort se borrarán y se volverán a crear otros con la configuración dada por el cliente.
Después de realizar esto es necesario volver a leer los archivos, darles el respectivo formato y colocarlos en el primer plano de la memoria para actualizarla.

- Dar Formato a archivos leídos
Se toman los datos del plano cero y se les aplica las operaciones necesarias para colocarlos con el formato establecido en el primer plano de la memoria. s importante saber que en caso de que haya datos previos en esta última parte de la memoria, en el momento en que se recibe esta instrucción se borran, sin posibilidad de recuperar.

Este módulo también registra las operaciones realizadas.

Salida de GSnort

Controla la salida de los datos generados por GSnort que se dirigen al cliente. Cualquier módulo de GSnort que le quiera enviar algo al cliente tiene que mandarlo primero a este módulo para que este lo envíe por el puerto correcto.

La manera de funcionar de este módulo es la siguiente:

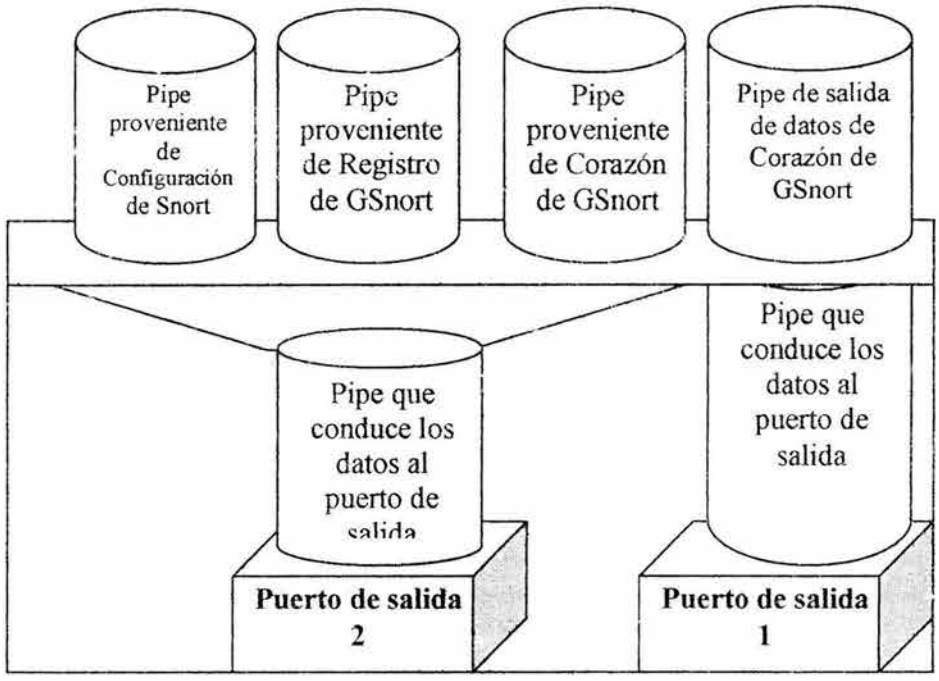

Figura D-5. Diagrama de la salida de GSnort

Existen tres 'pipes' que son dirigidos por el puerto de salida 2, los cuales mandan las respectivas respuestas a las peticiones de parte del cliente. A través de este puerto salen los paquetes de datos que se generan cuando el cliente pide algo específico a cualquier módulo del sistema GSnort Servidor.

Cada que llega algún paquete que se tenga que enviar al cliente por alguno de los 'pipes' dirigidos al puerto de salida 2, dicho 'pipe' se bloquea a los otros dos, después envía el paquete por el puerto de salida, luego lo desbloquea para que los demás puedan usarlo. Esto evita colisiones de datos en la salida.

Existe un 'pipe' que proviene del módulo 'Corazón de GSnort', el cual es redirigido hacia el puerto de salida 1. Por dicho 'pipe' circulan los datos generados por Snort al momento de analizar los paquetes de la red. Con esto el envío de datos es dedicado y optimizado.

Las instrucciones que puede recibir este módulo son las siguientes:

- Detener envío de datos de puerto de salida 1
Cierra la salida del puerto 1. Esto hace que el cliente no reciba datos, los elimina automáticamente.

- Detener envío de datos de puerto de salida 2
Cierra la salida del puerto 2. Esto evita que los datos que envían los tres módulos conectados a esta salida no sean enviados al cliente. Los datos no enviados se pierden.

Comandos de GSnort

Recibe las instrucciones provenientes del cliente, las analiza y las envía a cada uno de los módulos que correspondan.

Este módulo se conecta al módulo 'Pila de Comandos de GSnort', de aquí obtiene las instrucciones recibidas.

Una ves tomado una instrucción, procede a analizarla (averigua hacia que módulo va dirigido) y posterior a esto la envía a alguno de los otros 4 módulos. Esto se repite hasta que GSnort se detenga.

En caso de que no haya comandos enviados por el cliente, se mantiene en espera constantemente revisando la Pila de Comandos de GSnort hasta que exista un comando para analizar.

Solo analiza hacia quién va dirigida la instrucción y la envía, no verifica si es correcta.

Las funciones que este módulo lleva a cabo:

- Leer instrucción nueva
Lee una instrucción nueva de la Pila de Comandos de Gsnort. Si no lo existe, entra al modo de espera.

- Analiza la dirección y envía la instrucción
Verificar hacia que módulo va dirigida la instrucción y la envía.

- Modo de espera
En el momento en que no haya instrucción por analizar, queda en un estado de espera hasta que vuelva a existir alguna instrucción.

Registra todas y cada una de las operaciones que son ejecutadas. Se registra la hora de llegada, algunas características del cliente, hacia donde iba dirigida la instrucción, de que se trataba la instrucción y algunas otras características de la misma como el nombre y una pequeña descripción.

En conclusión, así como GSnort Servidor funciona como puente entre el cliente y el sistema Snort, este módulo, en conjunción con el módulo llamado 'Pila de Comandos de GSnort', funciona como puente entre el cliente y cada uno de los módulos del sistema GSnort.

Pila de Comandos de GSnort

Permite a GSnort poder responder a peticiones de manera ágil y en orden.

Hace las veces de una cola de espera[9] de las instrucciones que el cliente envía. Esto permitirá, en caso de que sean enviadas varias instrucciones de procesamiento tardado que no se puedan atender de manera rápida, que las instrucciones se esperen

mientras pueden ser atendidas por los otros módulos.

El siguiente diagrama define el funcionamiento de este módulo:

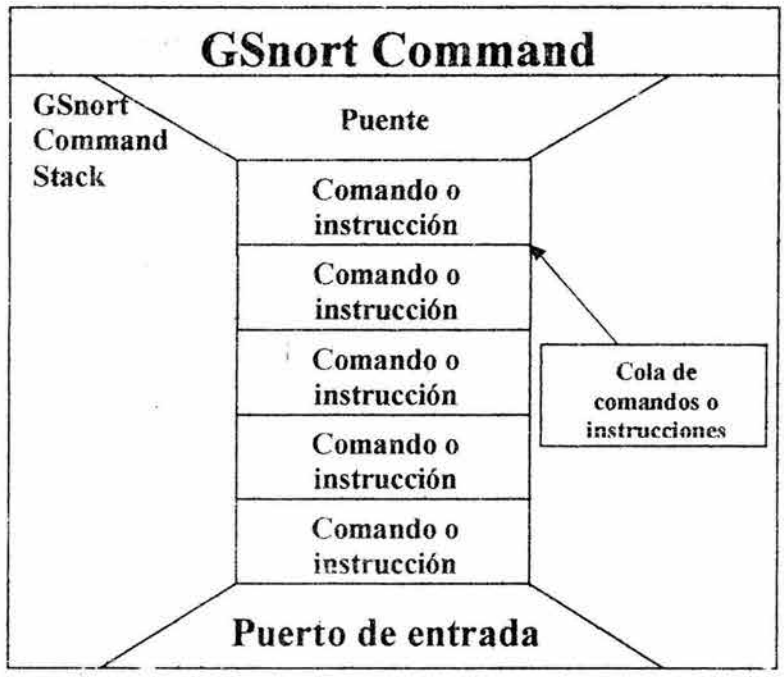

Figura D-6. Modo de funcionamiento de la pila de comandos de GSnort

Cada elemento de la cola de espera es de tipo 'comando'. Dichos elementos son enviados por el cliente, almacenados en la cola de espera y tomados posteriormente por el módulo 'Comandos de GSnort' para su futuro procesamiento.

Tiene sus propios métodos para manipular su contenido. Contiene dos funciones fundamentales, 'AgregarElemento' y 'ExtraerElemento', las cuales son usadas por la parte que recibe las instrucciones y por el módulo 'Comandos de Gsnort' respectivamente. Ni el primero puede leer la estructura de datos, ni el segundo puede insertar elementos en ella, esto para controlar el flujo de elementos dentro de la misma cola de espera.

Puertos de salida y entrada

GSnort contiene tres puertos, dos de salida y uno de entrada.

El puerto de entrada es aquel por el cual los clientes le envían peticiones a GSnort. A través de dichas peticiones, los clientes le indican las instrucciones respectivas para que GSnort trabaje como el cliente lo desea.

Los puertos de salida son los encargados de conducir los paquetes de datos al cliente. El puerto de salida 1 se dedica única y exclusivamente a enviarle los datos que Snort genera a través del análisis de paquetes, y los envía en tiempo real. El puerto de salida 2 se dedica a enviar las repuestas, generadas por los módulos de GSnort, a las peticiones hechas por el cliente. A través de este puerto los módulos pueden enviar los archivos de configuración, los archivos de registro de Snort, entre otras cosas.

Configuración del sistema GSnort

La configuración del sistema GSnort se realiza a través de archivos de texto con formato XML. Aquí se encuentran propiedades como los archivos donde se guardarán los registros de las operaciones que realiza cada módulo, los puertos de entrada y salida que se utilizarán, propiedades de estadísticas de GSnort, directorios de trabajo y de localización de los componentes, entre otras propiedades.

En el momento en que GSnort empieza a correr, toma este archivo, lo lee, adquiere todas las características, en caso de que no estén indicadas de manera explícita en el archivo GSnort las define con sus valores predeterminados, y conforme va levantando los diferentes servicios y módulos va proporcionándoles las características necesarias para que cada uno de ellos funcione correctamente.

Es importante que el administrador de GSnort construya de manera correcta estos archivos, porque de no ser así, GSnort podría realizar acciones que el administrador no quiera, y con esto perder un poco de su funcionalidad.

Apéndice E

Componentes de GSnort Cliente

Ya en el capítulo 5 se mencionaron los componentes de GSnort Cliente, en este apéndice se busca detallar el funcionamiento de cada uno de dichos componentes.

Para retomar un poco la estructura de GSnort Cliente se presenta la configuración de los componentes dentro de este mediante la siguiente figura (presentada en el capítulo 5):

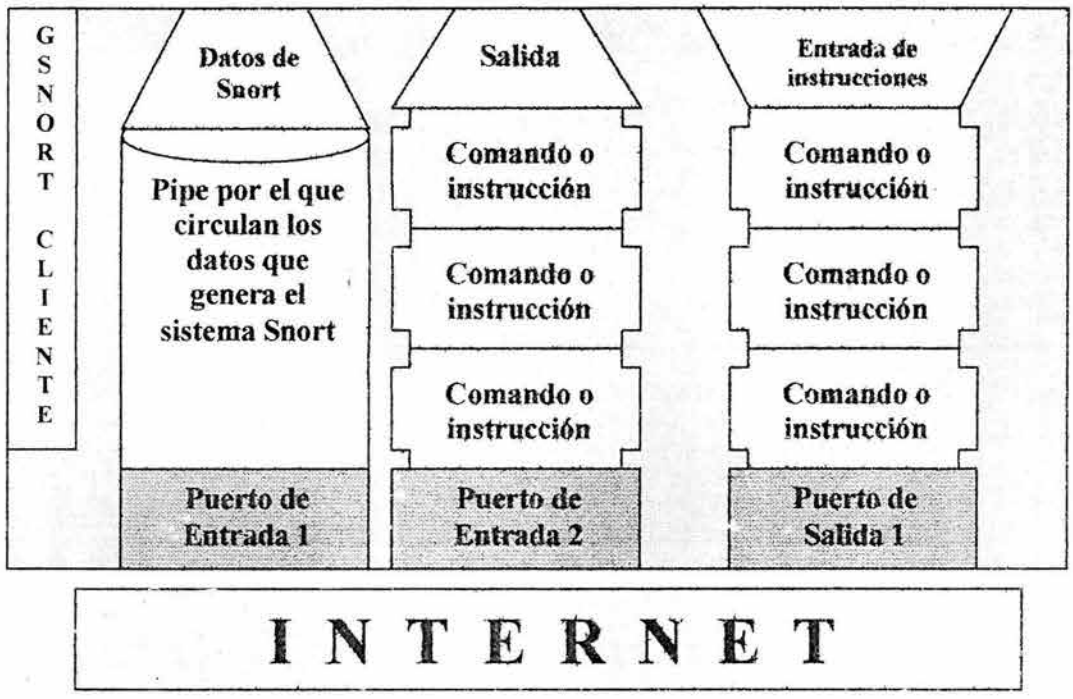

Figura E-1. Estructura de GSnort Cliente

A continuación se detallan cada uno de sus componentes:

Puertos de entrada

Son los puertos por los que GSnort Cliente se comunica a internet. A través de estos puertos, GSnort Servidor le envía los datos a este componente.

Por el primero puerto llegan los datos procesados por los módulos 'Corazón de GSnort', 'Configuración de GSnort' y 'Registro de GSnort'. Y por el segundo puerto llegan los datos el sistema Snort produce cuando alguna de las reglas estipuladas en la configuración es lanzada y genera alguna acción, alerta o registro, en contra del paquete que la causó.

De esta manera la interfaz puede usar un puerto dedicado exclusivamente para recibir los datos que el administrador de GSnort quiere ver en tiempo real, es decir los que son generados por Snort cuando este realiza alguna acción a causa de algún paquete. Y por otro lado, utilizará el otro puerto de entrada para recibir las

instrucciones o comandos que contienen los datos procesados por los diferentes módulos pertenecientes a GSnort Servidor.

Puerto de salida

El puerto de salida es dedicado para mandar instrucciones o comandos a GSnort Servidor. Cada que el cliente solicite algún tipo de dato o que le indique alguna instrucción a GSnort Servidor, es por aquí por donde se enviarán dichas instrucciones.

GSnort cliente abre, cuando inicia, una conexión a través de este puerto para mantener la comunicación con GSnort Servidor. Mientras que con los otros dos puertos usados los abre para mantener la comunicación en dirección contraria, es decir de GSnort Servidor a GSnort Cliente.

La interfaz de usuario, ya sea la perteneciente a GSnort o la que algún otro usuario realice, debe de enviar por este puerto[1] cualquier instrucción que quiera darle a GSnort Servidor, ya que este puerto es el que se encuentra conectado a la Pila de Comandos de GSnort, que es el módulo encargado de recibir las peticiones e instrucciones enviadas desde el cliente.

Pipe de datos

Es simplemente un 'pipe' de transición de datos, cuyas funciones son el de proporcionarle a los datos, que arriban desde GSnort Servidor, un canal de transporte para que la interfaz de usuario, a través de los plugins y los módulos, tome dichos datos y los pueda desplegar en algún lugar de la misma.

Simplemente es un transporte, no tiene ninguna puerta[2] que les impida el paso a los datos. Para que no transmita más datos es necesario enviarle una instrucción a GSnort Servidor indicándole que detenga la transmisión de datos hacia este puerto.

Esto resulta muy útil cuando GSnort Cliente queda en funcionamiento[3] pero la interfaz de usuario no se está usando, de esta manera no se transmiten datos de forma inútil.

Interfaz de datos de salida

Existen dos interfaces de datos de salida del componente[4], la que está conectada al 'pipe' de datos explicado en el punto anterior, y la que se conecta a la cola de espera de comandos recibidos, explicada en los siguientes puntos.

[1] Vale la pena aclarar que dicha interfaz no envía los datos directamente a través del puerto, sino que utiliza la interfaz conectada a la cola de espera de comandos de salida para enviar dichos datos, ya que con esto resulta más seguro y eficiente en el funcionamiento de este componente.
[2] Como un switch que permita el paso o la detención de los mismos datos.
[3] En modo background, es decir queda funcionando, sin que el usuario pueda verlo.

La interfaz que se encuentra conectada al 'pipe' de datos tiene la función básica de brindar, al módulo que lo desee, los datos que circulan por el mismo 'pipe'. Esta interfaz se crea con la finalidad de aislar el 'pipe', utilizado para la conducción de datos, de cualquier módulo fuera de este componente[5]. Esto evitará que algún módulo conectado a dicho 'pipe' lo cierre o cause algún error al mismo.

La interfaz que se encuentra conectada a la cola de espera de comandos tiene la función de permitir a la interfaz de usuario leer los comandos que llegan provenientes de GSnort Servidor. La ventaja que tiene esta es el que permite aislar dicha cola de espera de cualquier otro módulo externo a este componente. Esta interfaz tiene la peculiaridad que solamente permite leer la cola de espera a la que se encuentra conectada, por lo que evita un mal uso de esta última.

La única manera de acceder a la cola de espera de comandos y al 'pipe' de datos, que se encuentran en este componente desde el exterior del mismo es a través de estas dos interfaces. Con esto se logra una mayor seguridad en cuanto a la integridad del funcionamiento del componente GSnort Cliente.

Interfaz de datos de entrada

Esta interfaz se encuentra ligada a una cola de espera de comandos. Dicha cola de espera de comandos no es la misma que la cola de espera de comandos a la que se encuentra ligada la anterior interfaz. A diferencia de la anterior, esta cola de espera de comandos tiene la finalidad de almacenar los comandos o instrucciones que el GSnort Cliente envía a GSnort Servidor.

Esta interfaz permite la comunicación del exterior hacia dicha cola de espera. Esto permite un uso limitado y seguro de la estructura de datos.

La única operación que permite esta interfaz sobre la cola de espera es el agregar elementos a la misma, ya que es la única operación que una interfaz de usuario necesita para enviar las instrucciones o comandos a GSnort Servidor.

Esto evita malos manejos y errores en el funcionamiento de la cola de espera, con lo que se garantiza la integridad de la misma.

Cola de espera de comandos

Existen dos colas de espera de comandos. Ambos funcionan de la misma manera, almacenan los comandos o instrucciones que llegan a ella mientras que alguien más las lee. Esta estructura de datos es muy funcional para esta aplicación dada la arquitectura de la misma. Permite, en caso de un tráfico denso de comandos, que poco

[4] Es importante aclarar que cuando uno se refiere a salida del componente se quiere decir que los datos que se encuentran en un momento dado, por diversas circunstancias, dentro del componente saldrán del mismo, y se utilizará dicha interfaz para que algún otro componente los adquiera.

[5] Refiérase a GSnort Cliente.

a poco se vayan atendiendo todas y cada una de las instrucciones que llegan o se van.

La diferencia entre las dos estructuras de datos de este tipo que existen dentro del componente GSnort Cliente radica en que una es utilizada para la salida de comandos y la otra para recibir los mismos desde GSnort Servidor.

En el caso de la primera, su función es almacenar cada uno de los comandos que GSnort Cliente envía a GSnort Servidor, y en el momento en que se pueda, se envían a este último. La utilidad de esta estructura de datos se observa cuando por alguna razón[6] no se pueden enviar los comandos a GSnort Servidor, es entonces cuando esta estructura de datos los almacena hasta que se puedan enviar. Por un lado, el que se encuentra conectado a la interfaz de salida, solo permite la lectura o extracción de los elementos existentes en la cola de espera, mientras que por el otro lado, el que se encuentra conectada a internet a través del puerto de entrada 2, solo permite agregar elementos a la misma. De esta forma no hay problemas de integridad de datos en su funcionamiento, ya que solamente un agente agrega datos o elementos, y solamente un agente extrae los mismos.

En el caso de la segunda, su función es almacenar cada uno de los comandos que GSnort Cliente recibe de GSnort Servidor, y en el momento en que la interfaz de usuario pueda los lee de la cola de espera. La utilidad de esta estructura de datos se observa cuando por alguna razón[7] no se puede leer con la suficiente rapidez, por parte de la interfaz de usuario, los comandos que se encuentran llegando. Por un lado, la que se encuentra conectado a la interfaz de entrada, solo permite la escritura de elementos en la cola de espera, mientras que por el otro lado, la que se encuentra conectada a internet a través del puerto de salida, solo permite extraer los elementos para que sean enviados por internet hacia GSnort Servidor. De esta forma no hay problemas de integridad de datos en su funcionamiento, ya que solamente un agente agrega datos o elementos, y solamente un agente extrae los mismos.

[6] Que la conexión de internet se haya interrumpido, o que la conexión de internet es lenta, entre otras razones existentes.

[7] Que el procesamiento de algún comando que llegó sea muy robusto y esto retrase el procesamiento del siguiente. O cuando la interfaz de usuario esta ocupada en otros aspectos.

Bibliografía

Bibliografía

1. Doug Lea.
   Programación Concurrente en JAVA. Addison Wesley. 2001, España.
2. Mark Allen Weiss
   Estructura de datos en JAVA. Addison Wesley. 2000, España.
3. MohammadAkif, Steven Bordead, Andrei Cioroiaru, James Hart, Eric Jung, Dave Writz.
   Java y XML, Referencia para programadores. Ed. WROX. 2001, España.
4. Stephen Northcutt, Judy Novak
   Guía Avanzada de Detección de Intrusos, 2ª Edición. Prentice Hall. 2001, España.
5. Lenguaje de Programación JAVA. Sun Microsystem. Addison Wesley. 2001, Estados Unidos.

Referencias de Internet

1. http://www.snort.org – Página oficial del Sistema de Detección de Intrusos Snort
2. http://www.datanerds.net/~mike/snort.html - Página con información completa acerca del Sistema de Detección de Intrusos Snort.
3. www.cert.org – Página con información de Seguridad en Cómputo.
4. www.net-security.org - Página con información de Seguridad en redes de computadoras.
5. www.seguridad.unam.mx - Página con información de Seguridad en Cómputo de la UNAM
6. http://www.persystems.net/historia/internet.htm - Historia y evolución de Internet.
7. http://www.informaticahispana.com/~hackedplanet/Def_hack.htm - Definición de Hacker
8. http://www.sitiosargentina.com.ar/Help/diccionario%20tecnico.htm – Diccionario técnico de computación.
9. http://www.htmlweb.net/seguridad/tesis/tesis.html - Tesis doctoral sobre seguridad informática. Autor: Cristian F. Borghello.
10. http://www.tau.org.ar/base/lara.pue.udlap.mx/sistoper/ - Sistemas operativos.
11. http://www.redsegura.com/Temas/CRdefini.html - Definición de Criptografía.
12. http://www.rediris.es/cert/doc/unixsec/node26.html - Sistemas de detección de intrusos.
13. http://www.monografias.com/trabajos11/intru/intru.shtml - Sistemas de detección de intrusos.

Documentos

1. Documentos de la página http://www.snort.org; página principal del proyecto Snort.