UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"HERRAMIENTA PARA GESTIONAR INCIDENTES DE SEGURIDAD EN REDES"

T E S I S

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN

P R E S E N T A:

OSCAR ALEJANDRO LÓPEZ MELÉNDEZ

DIRECTORA DE TESIS:

ING. GLORIA GUADALUPE MARTÍNEZ ROSAS

MÉXICO, D.F. octubre de 2014

Agradecimientos

A mis padres:
Raúl Alejandro López Román y Adriana Meléndez Mendoza, por apoyarme en este camino que no fue fácil pero pudimos salir adelante, por su paciencia, cariño y por estar ahí en todo momento, pasamos por muchos momentos difíciles pero aquí estamos, también les agradezco la confianza que me brindaron para poder cumplir esta meta que les comparto, sin ustedes no se hubiera podido llegar hasta este punto y que hasta este momento me siguen apoyando. Gracias por esas palabras de aliento que me ayudaron a no darme por vencido y que lo importante es no mirar hacia atrás, sino de aprender de los errores y que sin ustedes no hubiera sido posible.

A mis hermanos:
Luis Alberto López Meléndez y Ariadna Gabriela López Meléndez, por todo su apoyo durante todo este tiempo, por sus palabras de aliento que me ayudaban a no darme por vencido y saber que la familia es la base más importante para poder lograr nuestras metas.

A mis sobrinos:
Diego Alexander y Brenda Sofía, por hacer mis días más alegres y hacer olvidar momentos difíciles, a ustedes les falta camino por recorrer y ahí estaré para apoyarlos.

A Viridiana Arias García:
Gracias por formar parte de esta nueva etapa que apenas inicia, gracias por tu amor, apoyo, cariño y confianza que tienes en mí, aún falta camino por recorrer y sé que ahí estarás.

A mis amigos:
Por el apoyo que me dieron durante los primeros años de la carrera, por las enseñanzas y buenos momentos.

A mi directora Gloria Guadalupe Martínez Rosas:
Por su apoyo en la realización de éste trabajo que sin su ayuda, orientación y experiencia no hubiera sido posible desarrollar.

Knowledge does not grow like a tree where you dig a hole, plant your feet, cover them with dirt, and pour water on them daily. Knowledge grows with time, work, and dedicated effort. It cannot come by any other means.

—Ed Parker, Senior Grand Master of American Kenpo

ÍNDICE

Introducción

INTRODUCCIÓN

Es de gran importancia que las organizaciones cuenten con sistemas de seguridad, confiables, eficientes y de gran utilidad, ya que diariamente existen ataques informáticos que cada vez tienen un mayor impacto y son más complejos, pudiendo con esto evadir diferentes mecanismos de defensa.

Sabemos que el problema principal para las organizaciones son los mismos usuarios, porque algunas veces aunque estén establecidas políticas de seguridad, éstos no las respetan y buscan la manera de burlar los sistemas del control de acceso, abriendo aquí un hueco que los atacantes podrían aprovechar.

Además, el auge de las redes sociales ha permitido que los atacantes puedan tener acceso a información valiosa de la organización, debido a que los usuarios en sus horas de ocio accesan a Facebook o Twitter, entonces ellos sin saber que les han enviado una URL maliciosa, dan clic a dicho enlace y es ahí cuando se efectúa el ataque por medio de una URL maliciosa. Existen diferentes tipos de ataques que utilizan los ciberdelincuentes entre los más comunes son DDoS (Denegación de Servicios Distribuido), defacement, que consiste en cambiar la apariencia del sitio web que está siendo comprometido, SQL Injection, Ingeniería Social, entre otros.

También es importante considerar que existen diferentes tipos de organizaciones delictivas o hacktivistas como se les suele llamar, lanzan campañas para atacar a una institución gubernamental o financiera, con la finalidad de comprometer información confidencial y así provocar que éstas tengan menos prestigio o confiabilidad hacia los clientes.

Por eso es importante contar con sistemas que faciliten la detección oportuna de alguna intrusión a la red interna de la institución, o conocer si alguno de estos grupos de ciberdelincuentes atacará a la institución, y poder con esto minimizar los ataques.

Es por eso que en este trabajo se habla de un proyecto que conjunte un detector de intrusos, un sistema que muestre la disponibilidad de los sistemas que están en la red interna y en específico en un área que es importante para las organizaciones llamado CeRT (Centro de Respuesta Temprana).

Este centro se encarga de notificar al área de seguridad informática si hay algún problema (intrusión, ataques a la red interna, etc.). También contar con un gestor de

respuesta a incidentes que sirve para el control de los eventos que se presenten en el CeRT y enviarlos al área de seguridad informática.

En el primer capítulo se hace mención de qué es un motor de búsqueda, objetivo y partes que lo componen; porque es el que servirá para conocer si hay noticias relacionadas con la organización.

También se habla de una aplicación que es útil para indicar si algún equipo que esté dentro del CeRT se encuentra disponible, se sabe que la disponibilidad es uno de los puntos principales dentro de lo que es la seguridad informática, y qué más si es un sistema que sirve para la detección de intrusos, si no se encuentra activo qué consecuencias traería esto a la organización.

El segundo capítulo habla de Security Onion, es una distribución Linux conformada por un IDS (Detection Intrusion) y un NSM (Network Security Monitoring), contiene un conjunto de aplicaciones que nos ayudan tanto en la detección de intrusos como en la interpretación de los mismos por medio de una interfaz web. Pero se necesita de mucha atención para la configuración mientras se realiza la instalación de Security Onion, porque si no se configura de manera correcta, las interfaces no podrán recolectar el tráfico que pasa por ellas.

En el tercer capítulo se explica acerca del detector de intrusos Snort y la interfaz web que ayuda para interpretar todos los datos que monitorea el Snort, existen otros como BASE, pero en este caso se utiliza Snorby que tiene una interfaz más atractiva para el usuario.

En el cuarto capítulo se habla de RTIR (Request Tracker for Incident Response), este gestor permitirá crear reportes de eventos o incidentes que se presenten dentro de la red interna de la organización, éstos se quedan almacenados, creando así una base de conocimiento para posteriores eventos que llegarán a presentarse, de la misma manera y con esto poder resolverlo más rápido.

Finalmente el quinto capítulo trata acerca de la aplicación de los capítulos tratados anteriormente puestos en práctica, en el cual se incluyen algunas demostraciones del funcionamiento de los cuatro módulos que se desarrollaron en este trabajo.

De esta manera se pretende conocer una herramienta que sería de utilidad para todas aquellas organizaciones que cuenten con un área dedicada a la seguridad informática,

y ayudando a todas aquellas pequeñas empresas a contar con lo mínimo de seguridad, si es que no cuentan con una herramienta que les auxilie a proteger su información.

En la conclusión, se determina por qué es importante contar con sistemas de seguridad como el que se trata en esta tesis, porque en la actualidad se ha notado más la actividad de esos grupos de ciberdelincuentes, por lo que las empresas deberían de tener una mayor y mejor protección.

En la bibliografía, se encuentran varias fuentes que son de utilidad, si se quiere conocer más a fondo sobre los temas tratados en esta tesis y que fueron necesarios para poder desarrollar el trabajo.

Capítulo 1

Motor de búsqueda de noticias referentes a seguridad informática y Ping Tester

CAPÍTULO 1

1.1 ¿QUÉ ES UN MOTOR DE BÚSQUEDA?

Los motores de búsqueda tienen una implementación muy compleja de software, el ejemplo de ello es Google que es experto proporcionando el acceso a toda la información que hay en internet.

Un motor de búsqueda implementa cuatro mecanismos básicos:

- Descubrir la manera en que encuentra los sitios en internet. Esto es posible con la ayuda de robots, estos robots lo que hacen es viajar por la web indexando contenido, los spammers lo utilizan también para escanear direcciones de correos electrónicos.
- Almacenamiento de enlaces, sumario de páginas, e información relacionada.
- Clasificación, utilizada para ordenar páginas almacenadas por su importancia.
- Entrega de resultados, se utiliza para organizar los resultados de la búsqueda basándose en la clasificación, en respuesta a una consulta de un usuario en específico.

La optimización de un motor de búsqueda puede ayudar a manejar más tráfico hacia un sitio web, por ejemplo si el sitio es de ventas lo importante será atraer a ese tráfico que contiene compradores potenciales o que les gusten las ofertas.

En nuestro caso lo que nos va a importar es atraer todo el tráfico de noticias referentes a seguridad informática o que contenga noticias que le sean importantes a la organización, como que aparezca su nombre en la lista de organizaciones que serán atacadas y poder así prevenir el posible ataque o aminorar el impacto que este podría tener a la institución.

Si la página tiene enlaces de sitios en un índice de búsqueda, Google u otro motor de búsqueda la encontraran más rápido.

Algunos motores de búsqueda indexan diferentes partes de la web. También en cualquier momento, eso es imposible para cualquier tipo de motor de búsqueda, indexar todo lo que se encuentra en la web.[1]

Cada una de las URL se introduce de manera manual al motor de búsqueda.

1.2 ¿CUÁL ES EL OBJETIVO DEL MOTOR DE BÚSQUEDA?

El objetivo de un motor de búsqueda es el de encontrar documentos o información que contenga las palabras clave introducidas[2], en este caso a un script. Normalmente localiza páginas web que coincidan con las palabras clave que se encuentran almacenadas en la base de datos, haciendo con esto más rápida la búsqueda de la información que necesitamos.

Los motores de búsqueda están diseñados para que, con solo escribir una palabra y hacer "clic", muestren la información que nos sea de interés, en este caso nos va a mostrar noticias o información que se relacione a la seguridad informática.

Las palabras claves son aquellas palabras que se utilizan para describir los conceptos o ideas que se buscan.

1.3 PARTES QUE COMPONEN EL MOTOR DE BÚSQUEDA

1.3.1 BASES DE DATOS (MySQL)

Para poder continuar con el script que implementará para la búsqueda de noticias enfocadas a la seguridad informática, se debe conocer primero que es una base de datos, para no hablar de los manejadores de bases de datos que existen, se explicará sólo en uno y va a ser el que se utilizará para desarrollar el motor de búsqueda, se habla de MySQL.

MySQL es un sistema administrativo relacional de bases de datos (RDBMS Relational Database Management System) por sus siglas en inglés, esto quiere decir, que puede ejecutar acciones como insertar, borrar registros o actualizar información, entre muchas otras cosas.

[1] (Davis, 2006)
[2] (Madrid, 2011)

Una base de datos relacional almacena datos en tablas separadas, en lugar de almacenarlo todo en grandes cantidades, esto añade velocidad y flexibilidad.
MySQL es multiusuarios, lo que le permite ser más rápido y robusto, es decir, que varios usuarios que se encuentren dentro de una red, pueden ejecutar diferentes tareas sobre la base de datos que se localiza en el mismo servidor.
Entre las empresas que utilizan este tipo de manejador se encuentran:

- Amazon: Tienda en línea más importante y grande del mundo.
- Cox Communication: La cuarta televisión por cable de E. U., tiene 3600 tablas y un aproximado de dos millones de inserciones cada hora.
- LiveJournal: Sitio de weblog que permite a los internautas mantener un periódico o diario en línea.
- Flickr: Gestiona millones de fotografías y usuarios con MySQL.
- NetQOS: Proporciona software y servicios de gestión de red, incluidas las aplicaciones para la gestión del rendimiento y análisis de tiempo de respuesta.
- Yahoo: Utiliza MySQL para las aplicaciones que maneja.
- Nokia: Utiliza un clúster MySQL para mantener la información en tiempo real sobre usuarios en redes móviles.
- Friendster: Es una red social de puros juegos en línea.
- Sabre: Proveedor líder en el mundo de soluciones que optimizan el desempeño del negocio a lo largo de toda la industria de viajes.
- Wikipedia: Sirve más de 200 millones de consultas y 1,2 millones de actualizaciones diarias, llegando a tener 11000 consultas por segundo.[3]

Este software MySQL proporciona un servidor SQL (Structured Query Language), está diseñado para entornos de producción críticos, con una alta carga de trabajo.
Algunas de las características más relevantes de MySQL son:

- Está escrito en C y C++.
- Está probado en un amplio rango de compiladores.
- Funciona en una amplia variedad de plataformas.

[3] (Sinemed, 2011)

- APIs disponibles para C, C++, Eiffel, Java, Perl, PHP, Python Ruby y Tcl.
- Usa tablas en disco B-tree (MyISAM) muy rápidas con compresión de índice.
- Soporte completo y funciones en las cláusulas de consultas SELECT y WHERE.
- Un sistema de privilegios y contraseñas que es muy flexible, seguro y que permite verificación basada en el host. Las contraseñas son seguras porque todo el tráfico de contraseñas está cifrado cuando se conecta con un servidor.
- Soporte a grandes bases de datos. Se utiliza MySQL Server con bases de datos que contienen 50 millones de registros. También se conoce a usuarios que usan MySQL Server con 60,000 tablas y cerca de 5,000,000,000,000 de registros.
- Los clientes pueden conectarse con el servidor MySQL usando sockets TCP/IP en cualquier plataforma. En sistemas Windows de la familia NT (NT, 2000, XP, o 2003), los clientes pueden usar *named pipes* para la conexión. En sistemas Unix, los clientes pueden conectar usando ficheros socket Unix.[4]

Entre muchas otras características.

MySQL es un sistema de gestión de bases de datos. Una base de datos es una colección estructurada de datos. Puede ser de cualquier cosa, desde una simple lista de compra a una galería de pintura hasta grandes cantidades de información en una red corporativa. Para añadir, acceder y procesar los datos almacenados en una base de datos, se necesita de un sistema de gestión de base de datos como MySQL Server.

MySQL cuenta con un servidor llamado MySQL Server, se desarrolló originalmente para tratar grandes bases de datos de una manera mucho más rápida y ha sido usado con éxito en entornos de producción de alto rendimiento durante varios años. MySQL Server ofrece hoy en día una gran cantidad de

[4] (MySQL, 2014)

funciones. Su conectividad, velocidad y seguridad hacen que MySQL Server sea altamente apropiado para acceder a las bases de datos que existen en Internet.[5]

1.3.2 SCRIPTS PHP

Un script es un programa que generalmente esta en texto plano y cada una de las líneas del programa son interpretadas en tiempo real, los script pueden estar dentro de un lenguaje de programación para hacer más funcional al script, uno de estos lenguajes es PHP.

Ahora bien PHP (Hypertext Preprocessor) por sus siglas en inglés, es un lenguaje de código abierto muy popular, especialmente adecuado para el desarrollo web y que puede introducirse en HTML.

La ventaja de ejecutar un script del lado del servidor, es que no hay problemas de accesibilidad que se podrían presentar en los scripts ejecutados del lado del cliente como JavaScript.

Para el desarrollo del motor de búsqueda se aplican dos scripts hechos en PHP, los cuales serán descritos para conocer cómo es su funcionamiento, y que el motor de búsqueda trabaje de la manera que se desea.

El primero de estos dos scripts es el que servirá para ir poblando la base de datos con las palabras clave y las URL que se necesiten, mientras que el segundo creará la interfaz de usuario para realizar las búsquedas. A continuación se explica cómo es que se crea la base de datos.

La base de datos para el motor de búsqueda consiste en tres tablas, cuyos nombres son: `page`, `word` y `occurrence`. La tabla de `page` contiene las páginas web indexadas, la tabla `word` almacena todas las palabras que encuentre en las páginas indexadas. Las filas en la tabla `occurrence` correlacionan las palabras que se encuentran contenidas en las páginas. Cada fila representa una ocurrencia de una palabra en particular sobre una página en específico.

[5] (MySQL, Panorámica del Sistema de Gestión de Base de Datos MySQL, 2011)

Mientras `page` y `word` mantienen los datos, `occurrence` funciona como una tabla de referencia. Para conjuntar las tres tablas, podrá determinar qué páginas contienen qué palabras, así como también cuantas veces la palabra se presenta.

Una vez que la base de datos fue creada, se podrá introducir el contenido que se necesita, en este caso las URL y las palabras clave, para esto se crea el script en PHP que toma una URL especificada por el usuario, obtiene las palabras clave y al mismo tiempo las va guardando dentro de la base de datos.

La base de datos se debe de conectar al host, junto con el nombre de usuario y su contraseña, después selecciona el nombre de la base de datos que se creó para almacenar las palabras clave y las páginas indexadas.

El script se conecta a la base de datos, registrando las páginas si es que no existen, y empieza a recabar los datos.

Existe una línea dentro del script que realiza la coincidencia de expresiones regulares, `preg_match_all ()`, extrae todas las palabras de la página, cada palabra se va guardando en las tablas de `word` y `occurrence`.

Cuando se construye el índice, solo es necesario utilizar la declaración en SQL `INSERT` que sirve para agregar registros a las tablas, cuando la página es indexada por primera vez debe ser agregada como sigue a continuación:

```
INSERT INTO page (page_url) VALUES ("http://www.algunapagina.com/");
```

Ahora la primera ocurrencia de una palabra dentro de todo el conjunto de datos se agregará así:

```
INSERT INTO word (word_word) VALUES ("palabra");
```

Cada ocurrencia de una palabra dentro de una página se registra de esta manera:[6]

[6] Fuente: Imagen 1.1, elaboración propia, 2014.

```
INSERT INTO occurrence (word_id, page_id) VALUES ('$word_id',
'$page_id');
```

Para poder ir indexando las páginas que son de interés referentes a la seguridad informática, se hace con la ayuda del script `poblar.php` de la siguiente manera:

```
http://localhost/poblar.php?url=http://www.algunapagina.com/
```

```
mysql> select * from page
    -> ;
+---------+-----------------------------------------------------
----+
| page_id | page_url
    |
+---------+-----------------------------------------------------
----+
|       4 | http://cert.inteco.es/cert/news/Noticias_CERT/
    |
|       8 | http://blogs.adobe.com/psirt
```

Figura 1.1. Contenido de la tabla page

Si se quiere revisar que efectivamente las paginas quedaron guardadas en la tabla de `page`, dentro del shell de MySQL se da la siguiente consulta (véase figura 1.1)

```
mysql> SELECT * FROM page;
```

El segundo script lo que va a implementar es, un formato HTML que va a realizar las consultas a la base de datos. Este va a trabajar como cualquier otro motor de búsqueda. El usuario introducirá en la caja de texto la palabra clave y dará enter, entonces recibirá el resultado de las páginas que contiene esta palabra.

El orden del resultado depende del número de veces en que aparece la palabra dentro de la página, también mostrará el tiempo que tarda en hacer la consulta.[7]

1.4 CONOCIENDO PING TESTER

Antes de hablar sobre las opciones que están dentro de la aplicación llamada Ping Tester, se explicará que es Ping Tester y cuál va a ser su funcionamiento dentro del proyecto.

[7] (Solin, 2002)

Ping Tester es una herramienta visual que prueba la disponibilidad de los sistemas que estén conectados al mismo servidor, puede almacenar una lista de direcciones IP, URL y comandos de prueba de la red para agilizar la eficiencia de trabajo. Ping Tester puede hacer una verificación con un solo clic. Con Ping Tester se puede hacer "ping sweep" (técnica usada para determinar que máquinas están activas en la red) a subredes o intervalos de pings a todos los host que están sobre una lista continua y el trazado o traceroute a una lista de host al mismo tiempo, pudiendo guardar los resultados en un archivo TXT o CSV.[8]

Ping Tester también es capaz de crear reportes estadísticos, especificando el intervalo de tiempo y poder así conocer el estado de las conexiones cada cierto periodo de tiempo.

1.4.1 PROGRAMACIÓN DEL ENVÍO DE PINGS A LOS SISTEMAS DEL CERT

Los ping pueden enviarse de manera automática programándolos. La programación automática permite especificar los días de la semana, meses, horas del día o cualquier intervalo de tiempo que se desee (véase figura 1.3)

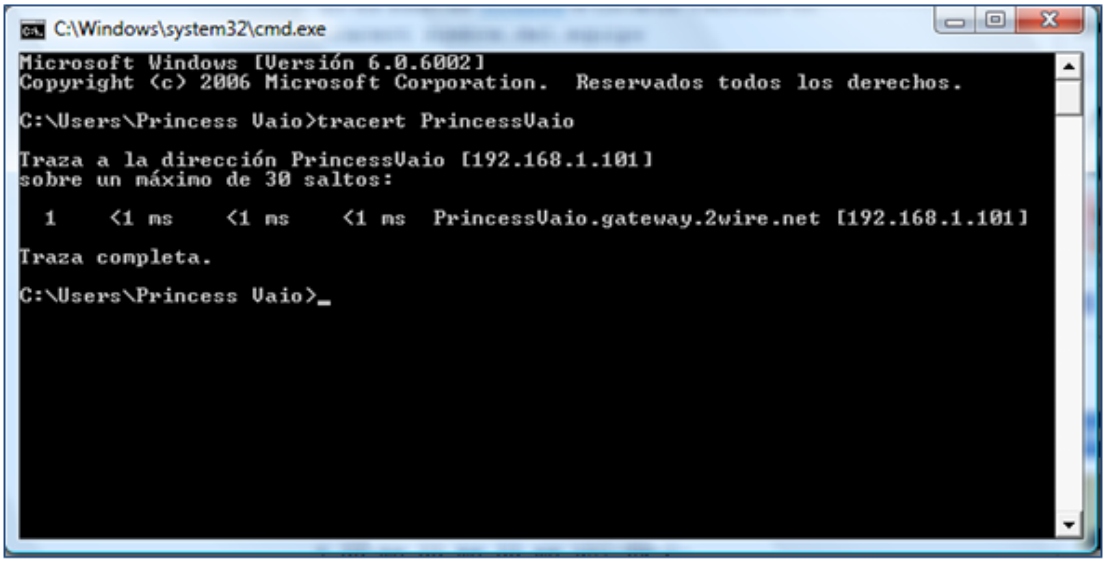

Figura 1.2. Traceroute en MS-DOS

[8] (AutoBAUP, 2013)

Este tipo de programación es de gran ayuda, porque permite estar al tanto de qué sistemas están activos o saber en qué momento del día quedó fuera de la red dichos sistemas.

También permite programar el *traceroute,* que permite conocer la ruta efectuada por un paquete y el tiempo en que tardan en llegar a su destino.[9]

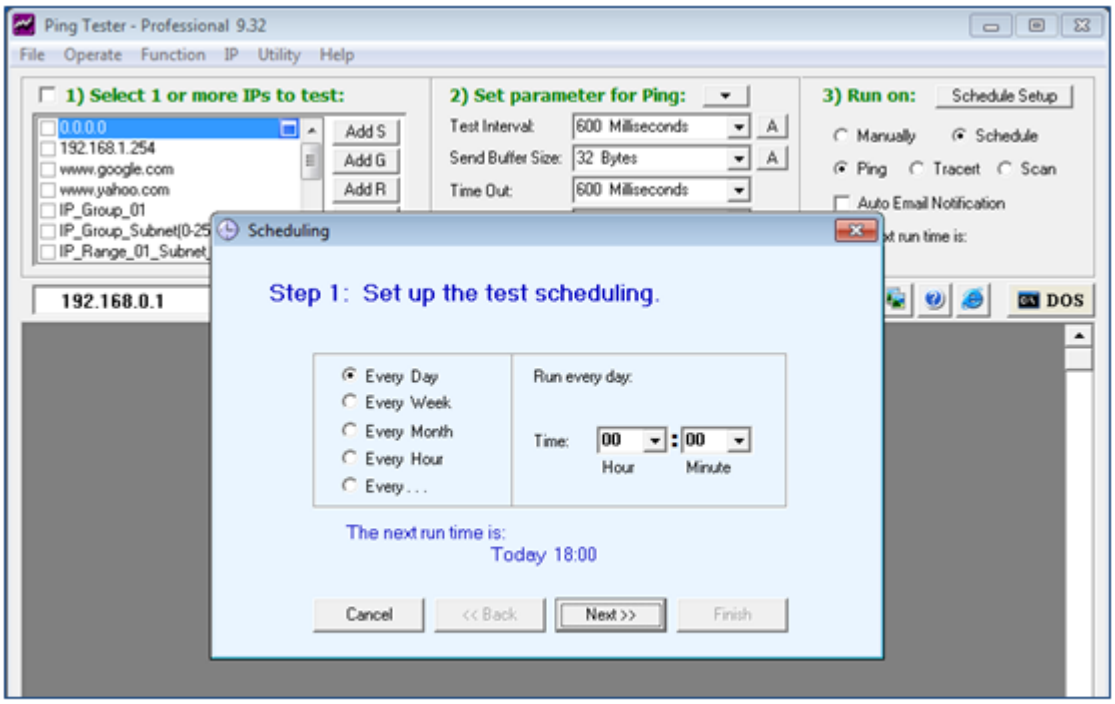

Figura 1.3. Programación del envío de pings con Ping Tester

Para evitar hacer scripts del comando (véase figura 1.2) y programarlo para que en un cierto periodo de tiempo realice el traceroute, Ping Tester será de gran ayuda.

[9] Fuentes: Imágenes 1.2 y 1.3, elaboración propia, 2014.

1.4.2 ENVÍO DE NOTIFICACIONES POR CORREO ELECTRÓNICO

Las notificaciones por correo electrónico permiten conocer el estado de la red en cualquier momento y en cualquier lugar. Los campos que se muestran en la imagen se deben de llenar conforme aparece en la cuenta que están creadas en Outlook (si es que se tiene una), Thunderbird entre otros, (véase figura 1.4), también se puede adjuntar el archivo con los resultados de la prueba para conocer más a fondo el estado de los sistemas que están dentro del CeRT.

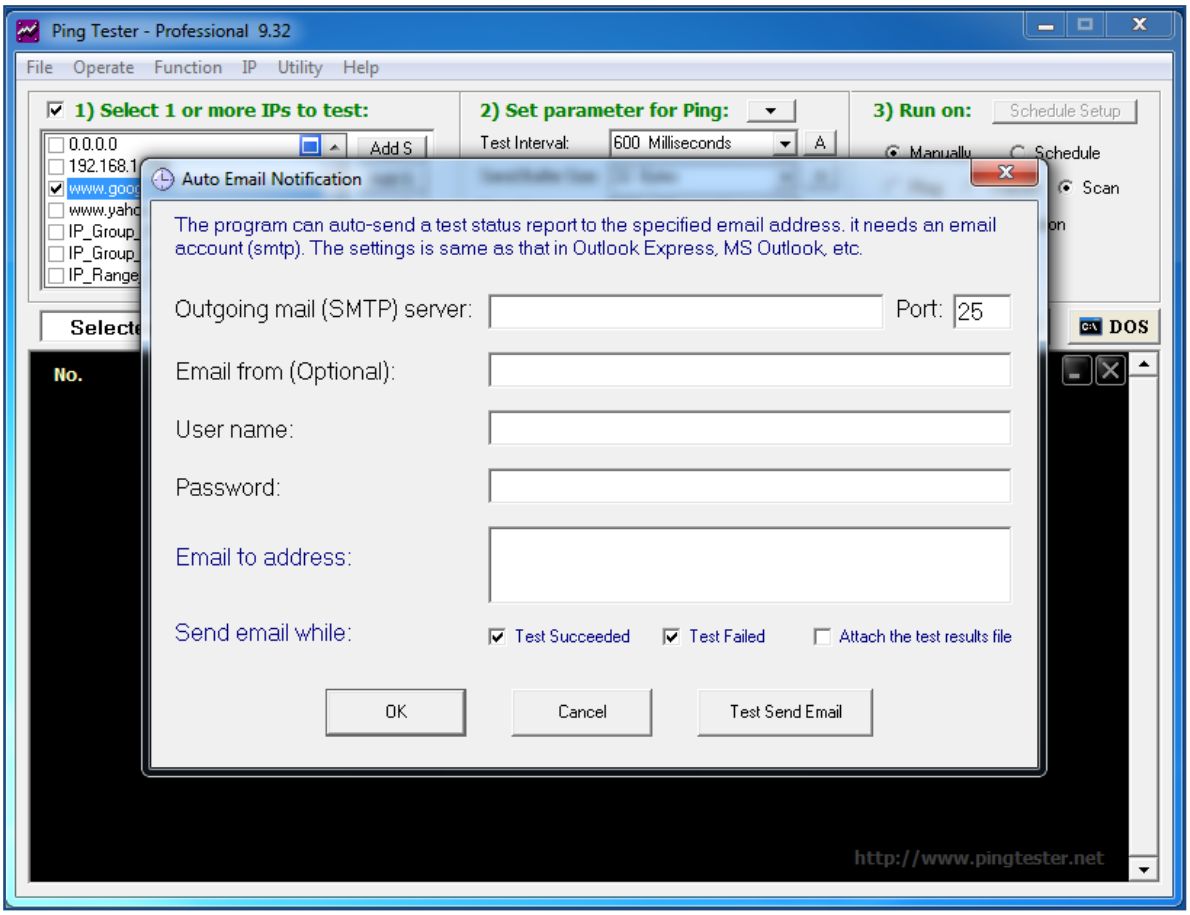

Figura 1.4. Auto-envío de un reporte del estado de los sistemas. Fuente: Ping Tester, 2014

1.4.3 ESTABLECER GRUPO DE IPs O URLs PARA CONOCER LA DISPONIBILIDAD

La función de IP Scanner, permite de una manera más rápida escanear un grupo de IPs para encontrar la dirección que se encuentra activa o no.

Se muestra encerrado en el círculo (véase figura 1.5), un grupo de IPs que serán escaneadas para ver si están activas o no, se puede introducir desde una IP hasta un conjunto de IPs dentro de un segmento.

En la parte inferior de la ventana de Ping Tester se muestra la respuesta de los pings hacia esas direcciones, es muy parecido a la consola de Windows, solo que en Ping Tester muestra la fecha y hora en que se está haciendo la solicitud.[10]

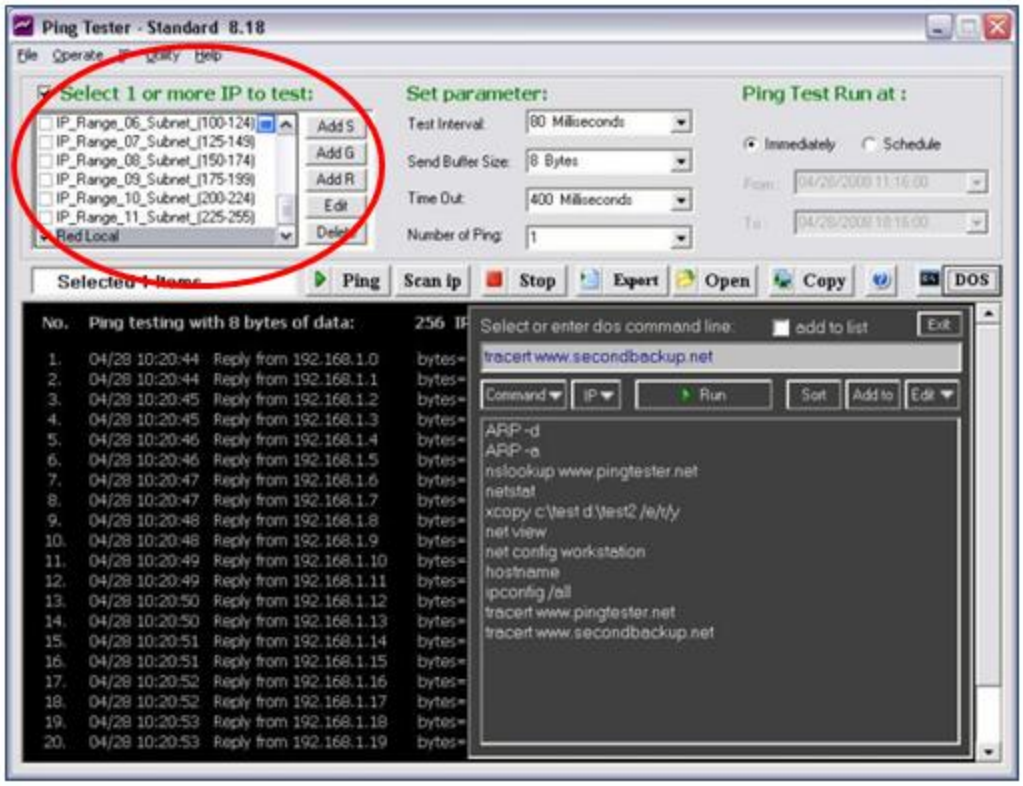

Figura 1.5. Grupo de direcciones IP

[10] Fuente: Imagen 1.5, elaboración propia, 2014.

También se puede ajustar el tiempo y el número de pings que se le quiera enviar a esas direcciones. Esta herramienta es sencilla pero es de mucha utilidad cuando se necesita conocer la disponibilidad de algunos sistemas que estén conectados a la red.

Capítulo 2

Sistema Linux Security Onion

CAPÍTULO 2

2.1 INSTALACIÓN

Ahora en este capítulo se realiza la instalación y configuración del sistema Linux llamado Security Onion, este sistema consta de un IDS (Intrusion Detection) y de un NSM (Network Security Monitoring), Security Onion está basado en Xubuntu 10.04.

Lo que se debe de realizar es la descarga de una imagen ISO vía http://sourceforge.net/projects/security-onion/files/12.04.3/ o vía Torrent. Esta imagen ISO se puede copiar a un DVD, después se reinicia la maquina donde se pretende instalar Security Onion, una vez reiniciada la máquina y con el Live DVD dentro aparecerá una ventana que mostrará las opciones para Security Onion.

Se muestran siete opciones (véase figura 2.1), la primera opción ejecuta el sistema sin instalarlo, teniendo las mismas opciones como cuando se está instalado en la máquina.

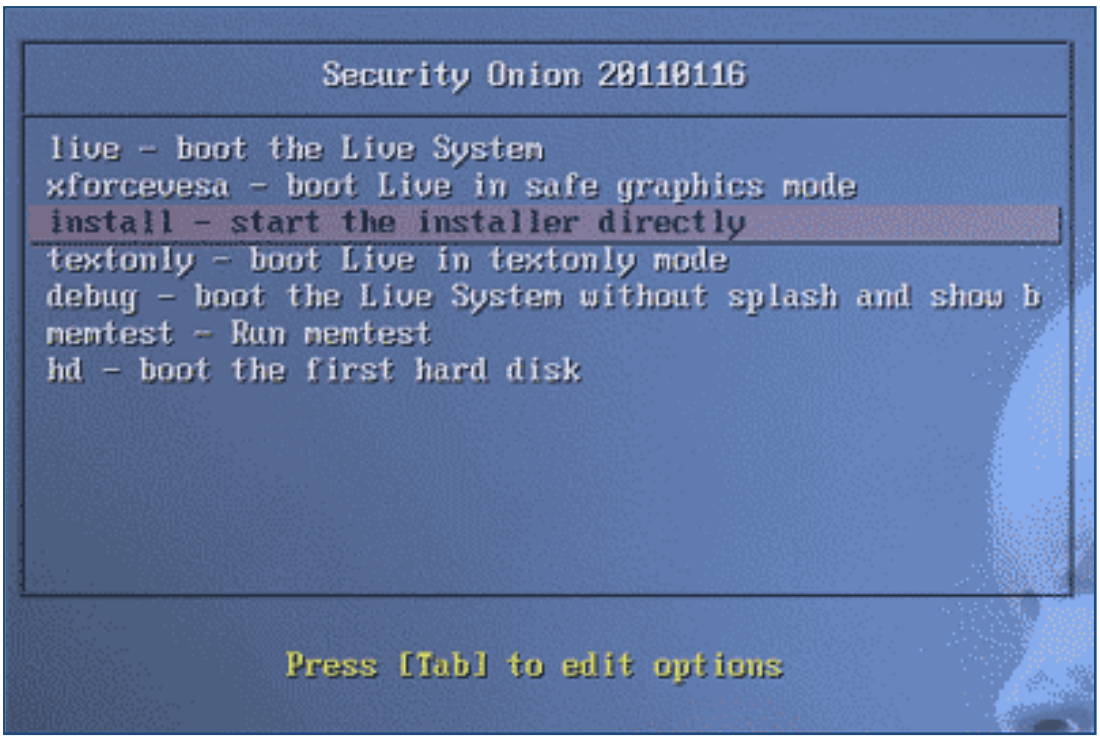

Figura 2.1. Opciones de instalación en Security Onion.
Fuente: http://secanalysis.com/security-onion-introduction-and-installation/

La segunda opción, es similar a la primera, sólo que aquí lo ejecuta en modo seguro, es decir, inicia el sistema únicamente con los controladores más importantes, deshabilitando de manera temporal alguna unidad interna o externa según su nivel de importancia dentro del sistema.

La opción de *Install* realizará la instalación dentro de la máquina, durante el proceso de instalación preguntará si se quiere que sea el único sistema operativo en la computadora o si quiere que conviva con el otro sistema operativo residente.

El resto de las opciones iniciará al sistema en línea de comandos, iniciará al sistema en texto plano o para realizar una prueba de memoria.

Las opciones se elegirán de acuerdo a las necesidades del usuario, en este caso se va a realizar la instalación dentro de un entorno virtual con la ayuda de VMware Workstation, el cual realiza la función de una computadora virtual sin afectar el sistema operativo residente.

Existen dos opciones para la instalación de Security Onion:

PRIMERA OPCIÓN

Si sólo se quiere una evaluación rápida de Security Onion usando una imagen ISO:

1. Se requiere por lo menos 1GB de RAM por cada interfaz de monitoreo de red, por lo que sería un total de 2GB de RAM porque se utilizarán 2 interfaces, una para monitorear y la otra que será un “sniffer”. Hay que tener en cuenta que los paquetes capturados podrían llenar el disco rápidamente, lo que se debe considerar es el tamaño de almacenamiento apropiado.
2. Descargar la ISO y hacer un Live DVD “booteable”.
3. Seleccionar la opción de *Install*.
4. Seguir las opciones de instalación.
5. Verificar la conectividad de internet, si se requiere la configuración de un proxy seguir lo siguiente:
    a. Los ajustes del servidor proxy están dentro de `/etc/enviroment`:

```
export http_proxy=https://server:port
export https_proxy=https://server:port
```

```
export ftp_proxy=https://server:port
export PERL_LWP_ENV_PROXY=https://server:port
```

6. Instalar las actualizaciones.
7. Hacer doble clic en el icono *Setup* que está en el escritorio, se abrirá un wizard que ayudara para la configuración de las interfaces, el directorio de las interfaces es `/etc/network/interfaces`, una vez hecho esto se procede a reiniciar la máquina.
8. Después de reiniciada la máquina, de nuevo doble clic en el icono de *Setup,* esto detectará si las interfaces fueron configuradas, después continuará con el resto de la configuración.
9. Una vez finalizado el wizard se podrán utilizar las aplicaciones que están en Security Onion, estas son Sguil, Squert, Snorby y ELSA.

SEGUNDA OPCIÓN

Si se requiere de una evaluación rápida de Security Onion sin sutilizar un ISO.

1. Se requiere por lo menos 1GB de RAM por cada interfaz de monitoreo de red, por lo que sería un total de 2GB de RAM porque se utilizaran 2 interfaces, una para monitorear y la otra que la hará de “sniffer”. Hay que tener en cuenta que los paquetes capturados podrían llenar el disco rápidamente, porque lo que se debe considerar el tamaño de almacenamiento apropiado.
2. Descargar un ISO de Ubuntu 12.04.
3. Seguir los pasos de instalación, durante el proceso de instalación preguntará por la opción de “encrypt home folder” se seleccionará “no habilite esta función”, también preguntará por actualizaciones automáticas, de igual manera se selecciona que “no se quiere habilitar las actualizaciones automáticas”.
4. Iniciar sesión con usuario y contraseña que se especificaron en el proceso de instalación.
5. Verificar la conectividad de internet, si se requiere la configuración de un proxy seguir lo siguiente:
    a. Los ajustes del servidor proxy están dentro de `/etc/enviroment`:

```
export http_proxy=https://server:port
export https_proxy=https://server:port
export ftp_proxy=https://server:port
export PERL_LWP_ENV_PROXY=https://server:port
```

6. Instalar actualizaciones.
7. Reiniciar:

```
sudo reboot
```

8. Configurar MySQL:

```
echo "debconf debconf/frontend select
noninteractive" | sudo debconf-set-selections
```

9. Agregar un repositorio estable a Security Onion:

```
sudo apt-get -y install python-software-
properties
sudo add-apt-repository -y
ppa:securityonion/stable
sudo apt-get update
```

10. Instalar el metapackage:

```
sudo apt-get -y install securityonion-all
```

11. Correr la configuración:

```
sudo sosetup
```

12. Seguir las instrucciones.
13. Analizar las alertas usando el cliente de Sguil o abriendo un navegador y poniendo `https://localhost`, por este medio se podrá accesar a Squert, Snorby y ELSA.[11]

[11] (Burks, 2013)

2.2 CONFIGURACIÓN

A continuación (véase figura 2.2) el escritorio una vez que Security Onion se instaló. Allí se puede ver el acceso directo para la configuración "s*etup*", éste nos permite la configuración de las interfaces y del NSM.

Figura 2.2. Escritorio de Security Onion.
Fuente: (Gupta, 2012)

Una vez que se le da doble clic a *setup* aparecerá una ventana (véase figura 2.3), en la cual se le dará continuar:

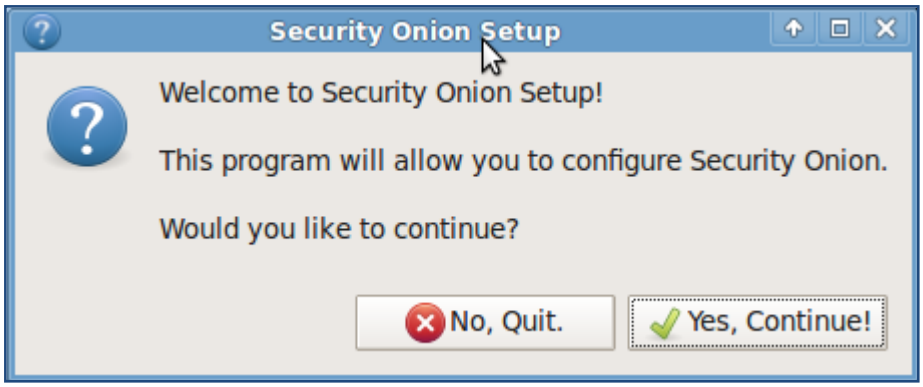

Figura 2.3. Bienvenida a Security Onion.
Fuente: (Gupta, 2012)

Después mostrará el tipo de configuración que se quiere realizar, en este caso se va a seleccionar *Advanced Setup* porque se tendrá mayor control de lo que se quiere para el sistema (véase figura 2.4)

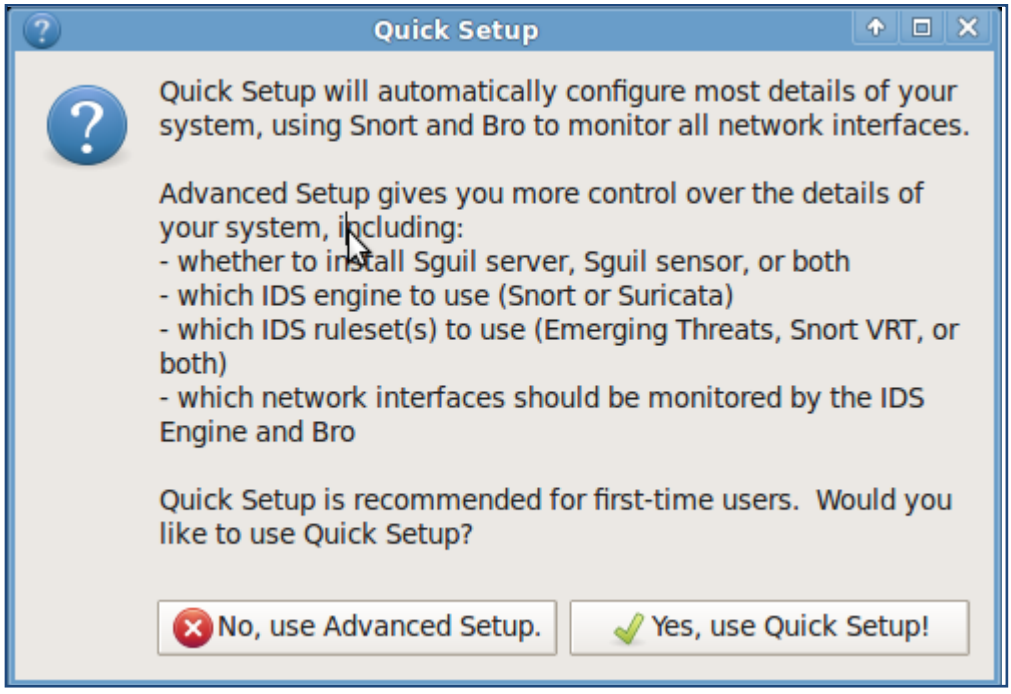

Figura 2.4. Selección de ajustes.
Fuente: (Gupta, 2012)

Ahora pedirá el tipo de IDS a usar (véase figura 2.5), entre ellos están Suricata y Snort, en este caso se seleccionará Snort.

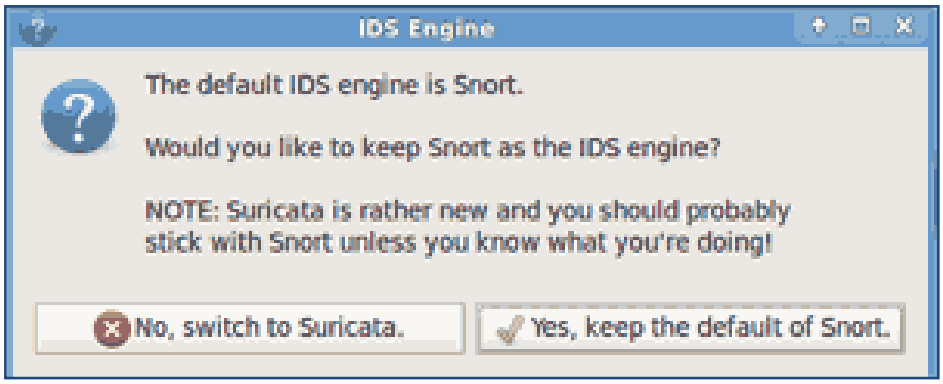

Figura 2.5. Selección de IDS.
Fuente: (Gupta, 2012)

Una vez elegido el IDS a usar se procede con la configuración de algunos componentes, que son el servidor y el sensor (véase figura 2.6)

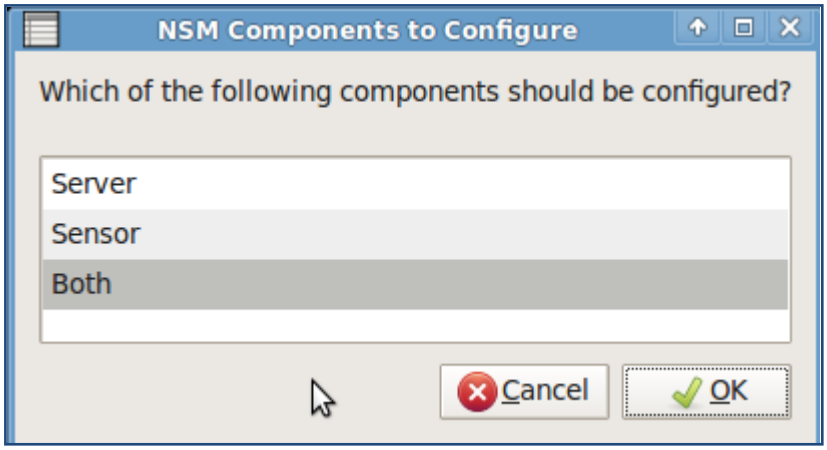

Figura 2.6. Selección del servidor y del sensor.
Fuente: (Gupta, 2012)

Si se selecciona la opción de *server* será porque la máquina estará en producción, es decir, se desplegará de manera distribuida, sólo que la máquina podrá correr únicamente Sguil, Squert, Snorby y ELSA por lo que no podrá monitorear las interfaces de red.

La opción de *sensor* se configura cuando ya se tiene el *server* instalado previamente, aquí se necesita habilitar el *ssh* (secure shell) para el *server* existente, con una cuenta que tenga privilegios de superusuario.

De otra manera seleccionar ambos y así poder configurarlos.

Lo siguiente es seleccionar las interfaces que estarán a la escucha de Snort (véase figura 2.7), se pueden seleccionar más de una interfaz.

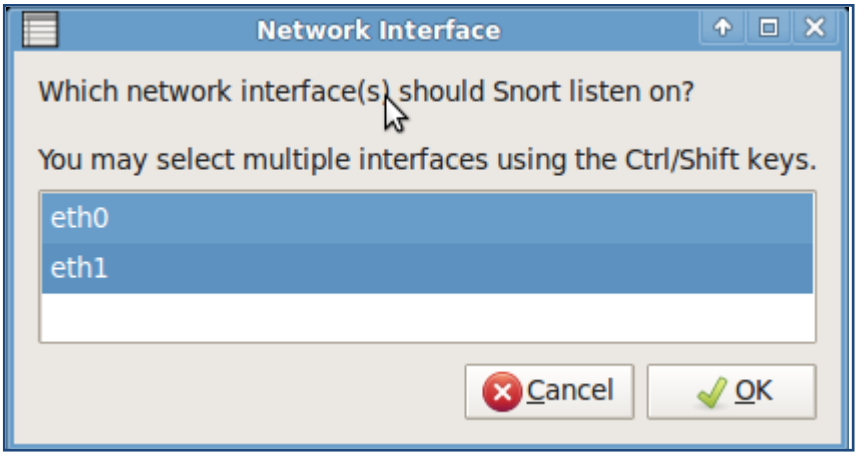

Figura 2.7. Interfaces de red.
Fuente: (Gupta, 2012)

Una vez seleccionadas las interfaces de red se continúa con la selección de las reglas, (véase figura 2.8) que utiliza Snort, para ver si existe algún problema dentro de la red que se va a estar monitoreando.

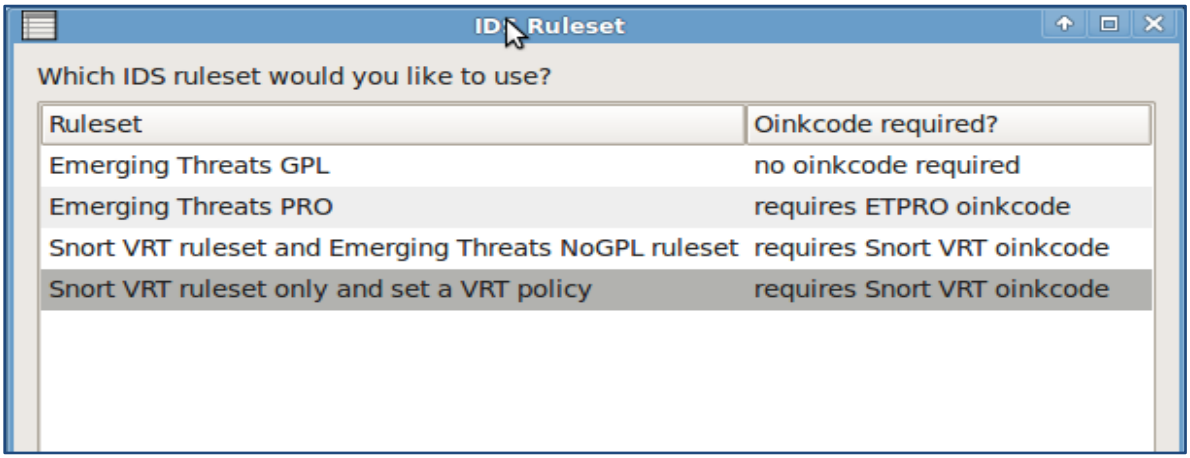

Figura 2.8. Selección del conjunto de reglas que utiliza Snort.
Fuente: (Gupta, 2012)

Se selecciona la primera opción ya que en las otras es necesario contar con un código, este código sirve para obtener las actualizaciones de las reglas antes de que se liberen para los demás usuarios.

Ahora se escribe el nombre de usuario que servirá para manejar las cuentas de Sguil y Squert (véase figura 2.9)

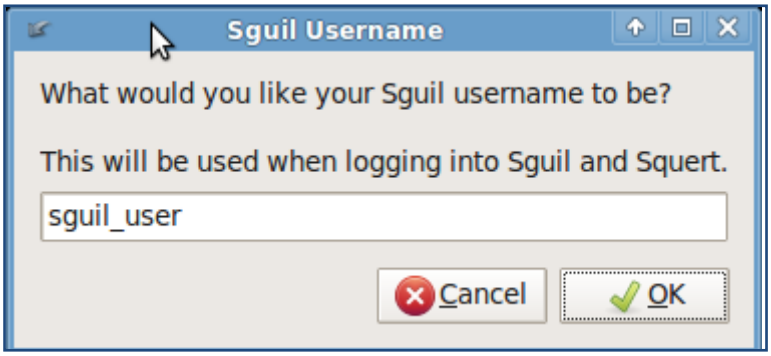

Figura 2.9. Usuario de Sguil y Squert.
Fuente: (Gupta, 2012)

Una vez colocado el nombre de usuario, ahora se coloca la contraseña que permitirá accesar a Snorby, Sguil y Squert (véase figura 2.10)

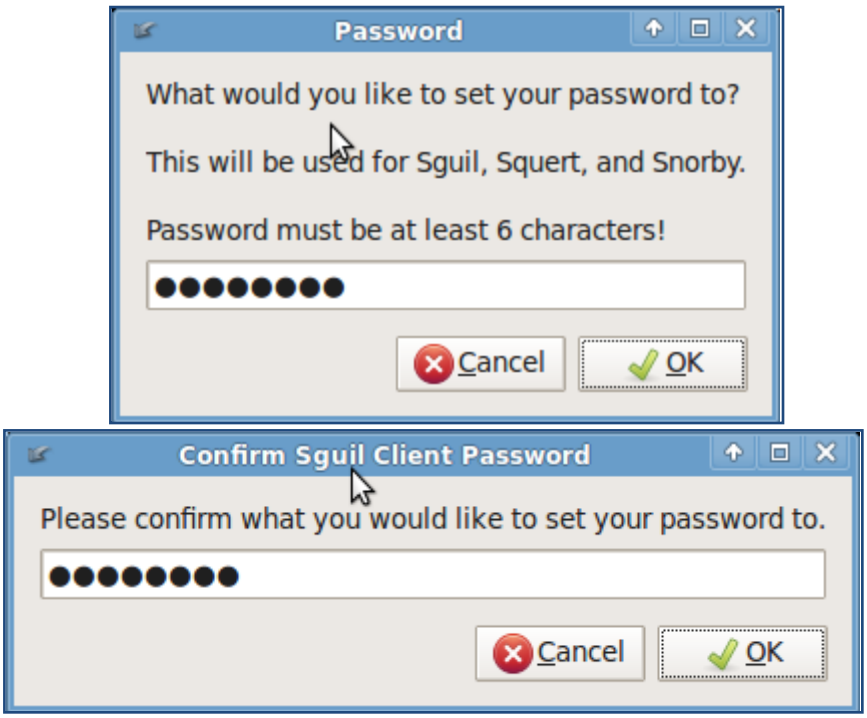

Figura 2.10. Selección y confirmación de la contraseña.
Fuente: (Gupta, 2012)

También se escribe el correo (véase figura 2.11) que servirá para poder utilizar Sguil y que también será de utilidad para que lleguen las notificaciones.

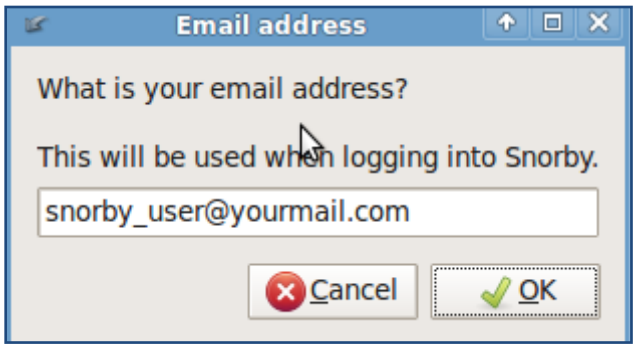

Figura 2.11. Correo para Snorby.
Fuente: (Gupta, 2012)

Una vez finalizado la configuración de Security Onion, muestra una ventana (véase figura 2.12) con la confirmación de la configuración, en este paso todavía se puede corregir alguna configuración que no se configuro como se desea, en caso contrario se selecciona "*si, proceder con los cambios*".

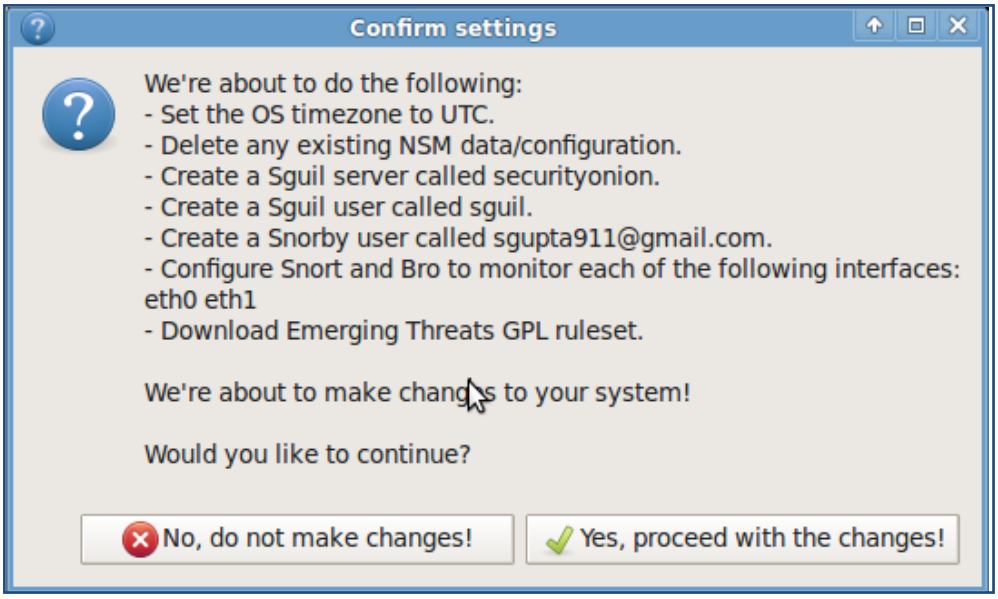

Figura 2.12. Confirmación de ajustes.
Fuente: (Gupta, 2012)

Por último muestra la ventana (véase figura 2.13) con los ajustes adecuados y la ubicación donde se encuentran las reglas de Snort, por si se requiere introducir algunas reglas personalizadas.

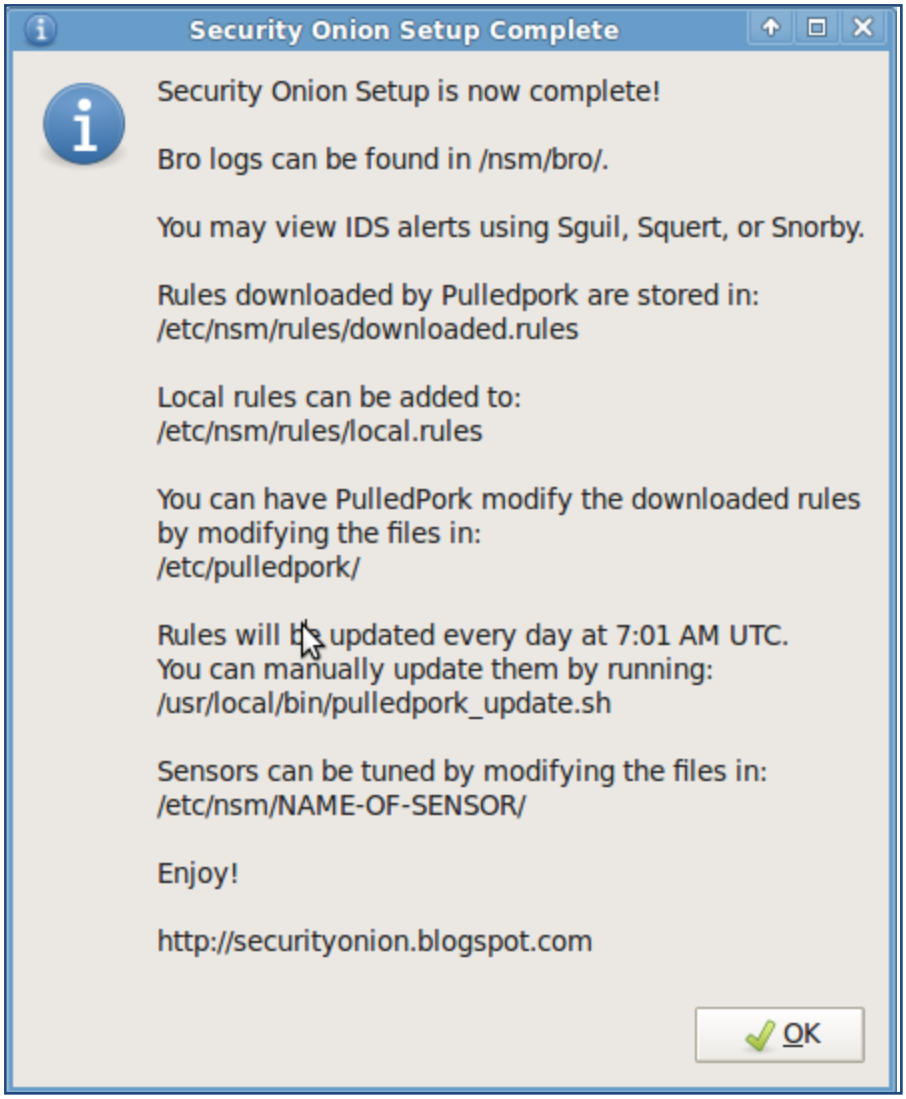

Figura 2.13. Ajustes configurados en Security Onion.
Fuente: (Gupta, 2012)

Para iniciar, detener o reiniciar el servicio del NSM (Network Security Monitoring), desde la línea de comando se puede escribir lo siguiente:

```
$ sudo service nsm start|stop|restart
```

2.3 APLICACIONES QUE LO COMPONEN

Security Onion está compuesto por otras herramientas que permiten conocer a detalle si algo no anda bien en la red, estas aplicaciones o herramientas adicionales son Squert, Sguil, Snorby, Snort y ELSA.

2.3.1 SQUERT

Es una aplicación web que es utilizada para consultar y ver los datos almacenados en la base de datos de Sguil. Squert es una herramienta visual (véase figura 2.14) que proporciona un contexto adicional de eventos a través del uso de metadatos, la representación de series de tiempo y los conjuntos de resultados, se agrupan de manera lógica.[12] La nueva versión de Squert está completamente escrita en JavaScript.

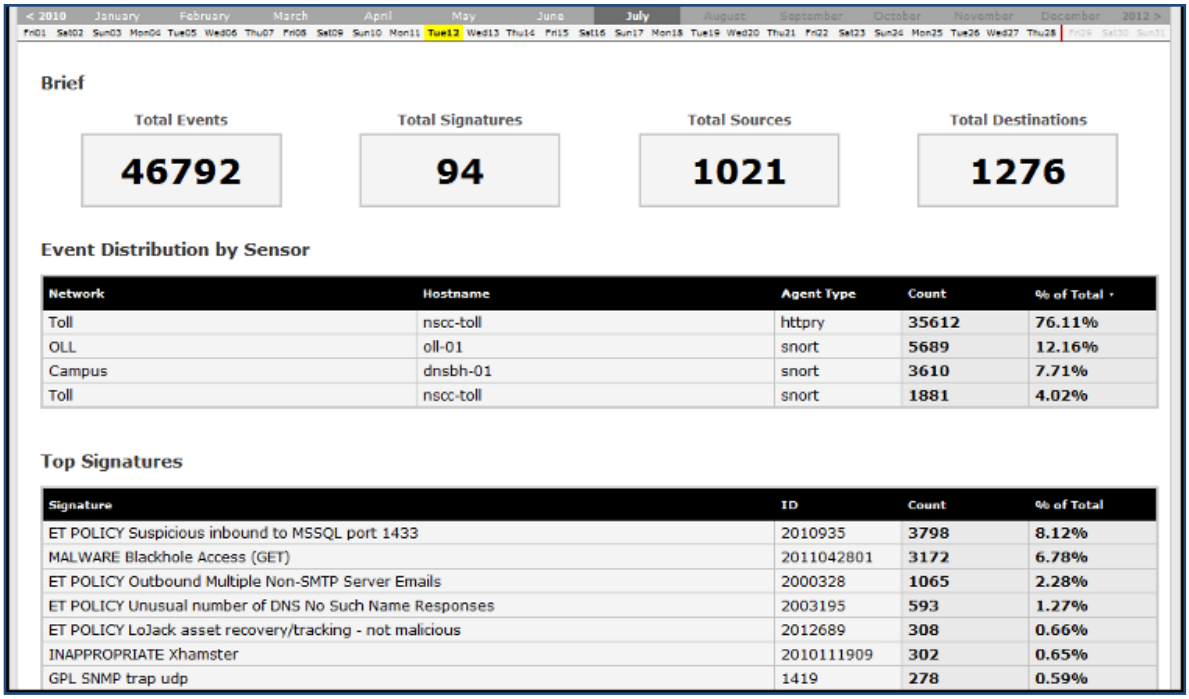

Figura 2.14. Interfaz de usuario de Squert.
Fuente: (Project, 2013)

[12] (Project, 2013)

2.3.2 SGUIL

Es una colección de componentes de software libre para los NSM y dirige el análisis de eventos de las alertas de un IDS. Está construido por analistas de la seguridad de la red para analistas de seguridad de la red.[13]

El componente principal de Sguil es una interfaz intuitiva que permite el acceso en tiempo real a los eventos, a la sesión de datos y a la captura de paquetes. Sguil facilita la practicidad del monitoreo de seguridad de la red y al manejo del análisis de eventos.

La arquitectura de Sguil está compuesta de un servidor y de un número cualquiera de sensores en red. Los sensores desempeñan la tarea del monitoreo de seguridad.

El servidor coordina la información recabada por los sensores, esa información es almacenada en una base de datos, se comunica con el cliente que está siendo ejecutado sobre el escritorio de la máquina del administrador.[14]

Cada sensor monitorea un simple enlace de red (puede contar con múltiples sensores sobre una maquina física). Estos sensores recolectan diferente tipo de información:

1. Snort monitorea el enlace de eventos de seguridad y los registra en un archivo que se guarda en el disco local.
2. Barnyard toma los eventos del archivo de registros de Snort y los envía al sensor, el cual inserta esos eventos a la base de datos que está corriendo sobre el servidor de Sguil en tiempo real.
3. Una instancia independiente de Snort registra el contenido completo de todos los paquetes de la red en el disco local lo cual, va a requerir de una gran partición de datos.
4. SANCP registra sesiones TCP/IP y las envía a la base de datos que está en el servidor de Sguil.
5. Sguil también está a la escucha de los comandos del servidor. Estos comandos son normalmente las solicitudes de los paquetes que han sido registrados por Snort.

[13] (Sguil, 2014)
[14] (Wikipedia, 2013)

A continuación se muestran (véase figura 2.15) los puertos más comunes que utiliza Sguil en su versión 0.7.0.

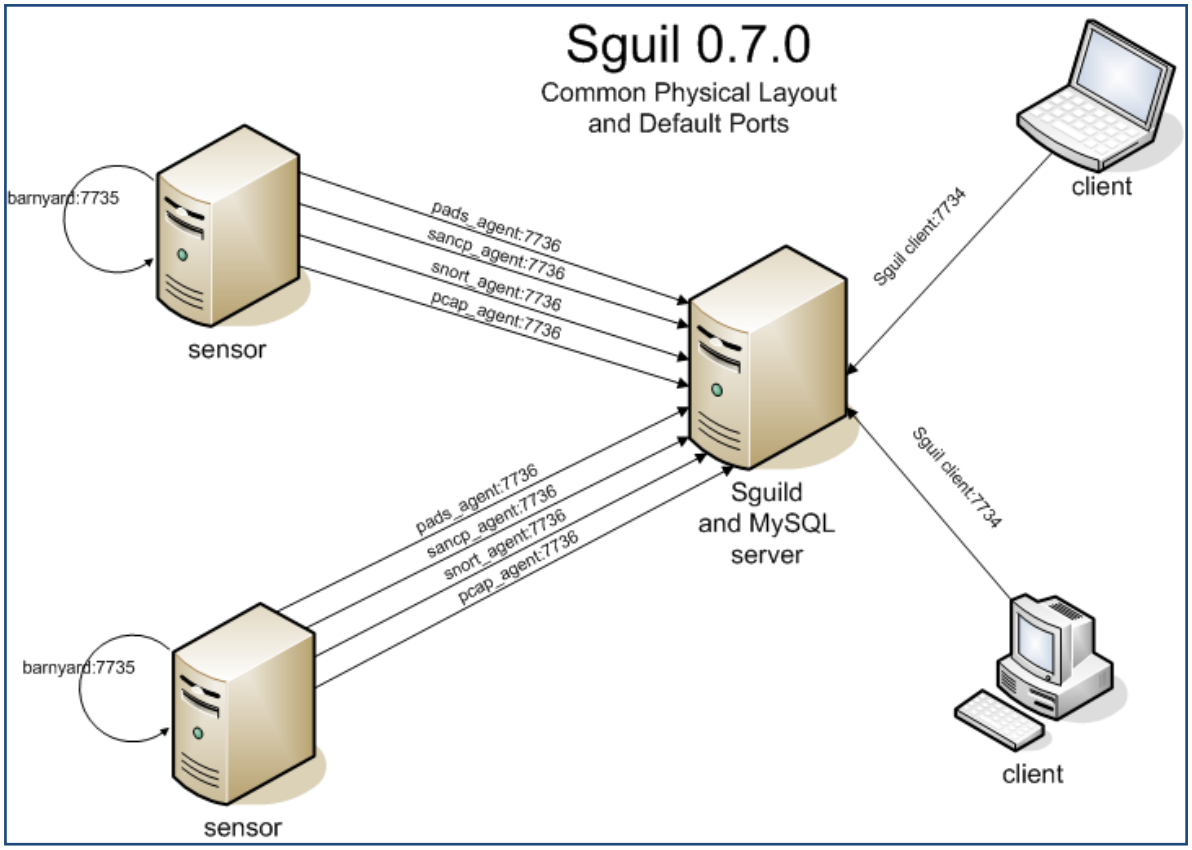

Figura 2.15. Configuración de Sguil.
Fuente: (Gupta, 2012)

Para la configuración del servidor de Sguil se va a utilizar la base de datos que se creó al inicio de la configuración del NSM. La ruta del archivo de configuración se ubica en `/etc/sguild/server.conf` lo que va a permitir la personalización de la base de datos de Sguil. La variable `DAYSTOKEEP` en el archivo de configuración `/etc/nsm/securityonion.conf` permite ajustarlo a un periodo de retención para las alertas en la base de datos de Sguil.[15] Los servicios de infraestructura del NSM se inician con `service nsm start.` A continuación se muestran (véase figura 2.16) todos los servicios iniciados.

[15] (Gupta, 2012)

Una vez que los servicios están iniciados, el cliente Sguil puede ser lanzado. Sguil (véase figura 2.17) permitirá seleccionar cuál de las interfaces de red va a monitorear (eth0, eth1 y ossec). Se da clic en `Select All`, esto permitirá mostrar las alertas.

```
user@orionvm:~$ sudo service nsm start
Starting: securityonion
  * starting: sguil server                                              [  OK  ]
Starting: orionvm-eth0
  * starting: pcap_agent (sguil)                                        [  OK  ]
  * starting: sancp_agent (sguil)                                       [  OK  ]
  * starting: snort_agent (sguil)                                       [  OK  ]
  * starting: snort (alert data)                                        [  OK  ]
  * starting: barnyard2 (spooler, unified2 format)                      [  OK  ]
  * starting: sancp (session data)                                      [  OK  ]
  * starting: pads (asset info)                                         [  OK  ]
  * starting: pads_agent (sguil)                                        [  OK  ]
  * starting: daemonlogger (full packet data)                           [  OK  ]
  * starting: argus                                                     [  OK  ]
  * starting: httpry                                                    [  OK  ]
  * starting: httpry_agent (sguil)                                      [ OK ]
Starting: orionvm-eth1
  * starting: pcap_agent (sguil)                                        [  OK  ]
  * starting: sancp_agent (sguil)                                       [  OK  ]
  * starting: snort_agent (sguil)                                       [  OK  ]
  * starting: snort (alert data)                                        [  OK  ]
  * starting: barnyard2 (spooler, unified2 format)                      [  OK  ]
  * starting: sancp (session data)                                      [  OK  ]
  * starting: pads (asset info)                                         [  OK  ]
  * starting: pads_agent (sguil)                                        [  OK  ]
  * starting: daemonlogger (full packet data)                           [  OK  ]
  * starting: argus                                                     [  OK  ]
  * starting: httpry                                                    [  OK  ]
  * starting: httpry_agent (sguil)                                      [ OK ]
Starting: HIDS
  * starting: ossec_agent (sguil)                                       [  OK  ]
```

Figura 2.16. Inicio de servicios del NSM.
Fuente: (Gupta, 2012)

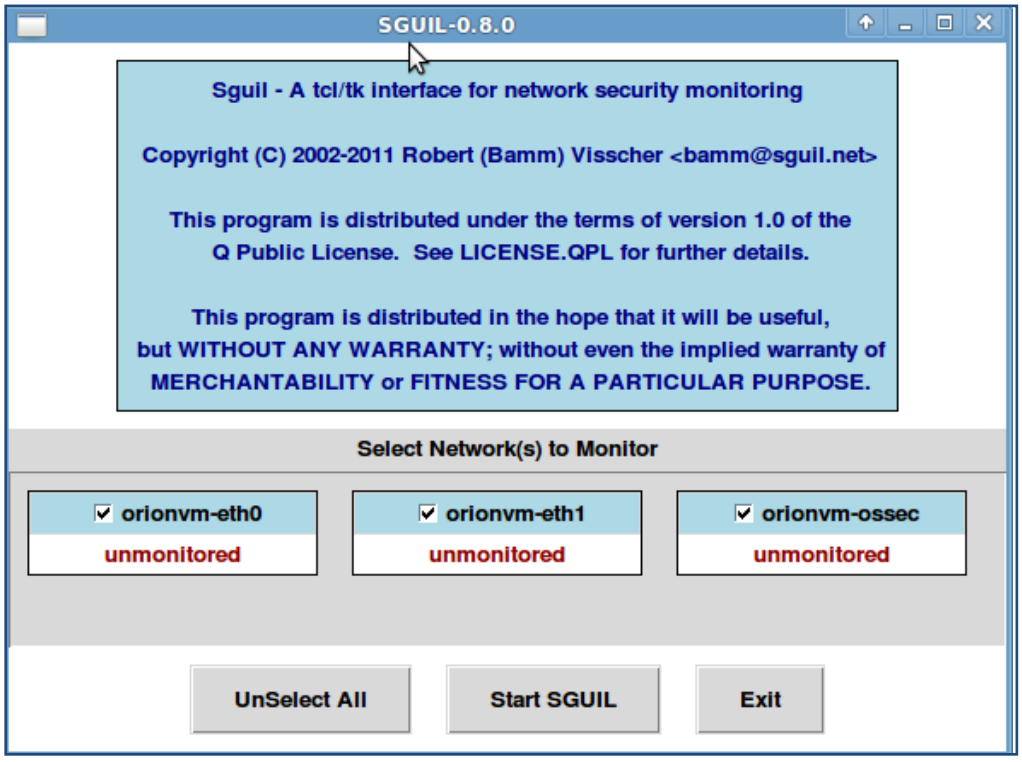

Figura 2.17. Selección de interfaces.
Fuente: (Gupta, 2012)

2.3.3 SNORT

En esta parte se habla acerca de lo que es Snort y los elementos que son importantes considerar para su correcto funcionamiento, todo esto a grandes rasgos.

Si bien Snort es un sistema de código abierto que consiste en la detección y prevención de intrusos (IDS/IPS) por sus siglas en inglés, desarrollado por Sourcefire.[16]

Combina los beneficios de firmas, protocolos e inspección basados en anomalías.

Snort no es difícil de utilizar, lo que tiene es que trabaja sobre línea de comandos y hay que tener en cuenta que no siempre es obvio qué comandos van con qué otros comandos.

Snort puede ser configurado para correr en 3 modos:

- Modo *sniffer*, este modo simplemente lee los paquetes que están fuera de la red y los muestra en una trasmisión continua en la pantalla.
- Modo *packet logger* , registra los paquetes en el disco.
- Modo *Network Intrusion Detection System (NIDS)*, interpreta la detección y análisis del tráfico que esta sobre la red, este modo es el más complejo y configurable.

Snort consiste en una serie de reglas que ayudan para la detección de intrusos, las reglas necesitan ser personalizadas para reducir el número de falsos positivos, hay dos maneras para escribir las reglas y poder distinguir un registro basado en eventos.

El análisis puede optimizarse para una mayor eficiencia y facilitar la manera de escribir una regla para alertar al sensor LIDS que está basado en su experiencia.

El sensor NIDS trabaja con reglas de Snort para alertar algún evento sobre la red de interés. Escribir las reglas se convierte en la parte más importante y sin duda la más difícil, porque esto es lo que va a permitir supervisar la seguridad de la red (Gupta, 2012)

[16] (Gupta, 2012)

2.3.4 SNORBY

Snorby es una aplicación web front-end (escrita en Ruby on Rails) para cualquier aplicación que registre eventos en formato de salida binario unified2. Snorby se integra con un sistema de detección de intrusos como Snort, Suricata y Sagan. El concepto fundamental dentro de Snorby es simple y poderoso. El objetivo del proyecto es crear una aplicación altamente competitiva, que sea de código abierto y libre para el monitoreo de las redes, ya sea para uso privado o uso empresarial (Gupta, 2012)

Algunas de las características de Snorby se mencionan a continuación:

- Métricas y reportes: Comparte datos como comparaciones de actividad del sensor o de sus firmas más activas directamente con los informes diarios, semanales, mensuales y reportes ad-hoc en PDF.
- Clasificación: Con un simple golpe de teclado o un simple clic, puede rápidamente clasificar un evento dentro de una de las muchas clasificaciones pre configuradas o dentro de una clasificación personalizada, que sea relevante para la organización. Utilizar clasificaciones para organizar eventos son de gran ayuda para darle seguimiento a investigaciones o afinar el conjunto de reglas.
- Paquetes completos: A diferencia de la mayoría de las aplicaciones de monitoreo de seguridad de red, Snorby está integrado dentro de una nueva y existente instalación de OpenFPC, Solera DS Appliances y Solera's DeepSee para dar un completo análisis de los paquetes y sesión de datos.
- Ajustes personalizados: Mientras Snorby está diseñado para trabajar fuera de la caja, es el lanzamiento más configurable hasta la fecha. Añade severidades o clasificaciones personalizadas, gestiona las notificaciones de correo electrónico e incluso amplía la funcionalidad con productos de terceros.
- Acceso rápido: Snorby funciona con aproximadamente 20 accesos rápidos permitiendo a los analistas para navegar, ver y clasificar eventos sin el uso del mouse. Esto le da a los analistas la respuesta y eficiencia de un cliente, instalado dentro de la simplicidad y la facilidad de un navegador web.

- Código abierto: El código fuente de Snorby está disponible bajo la versión 3 de la licencia permisiva de GNU. Snorby utiliza tablas para las métricas y reportes, cuenta con su propia concesión de licencias.[17]

2.3.5 ELSA

Enterpise Log Search and Archive (ELSA), es un marco de syslog centralizado, construido sobre Syslog-NG, MySQL y Sphinx de búsqueda de texto completo. Proporciona un interfaz (véase figura 2.18) de consulta, basado en web totalmente asíncrono que normaliza los registros y hace la búsqueda de miles de millones de registros por cadenas arbitrarias sea tan fácil, como buscar en la web.

ELSA está integrada en Security Onion, porque incluye herramientas para la asignación de permisos para ver los registros, así como alertas de correo electrónico, consultas programadas y gráficas.

Algunas de las funciones con las que cuenta ELSA son:

- Alto volumen de recepción/indización (un simple nodo puede recibir arriba de 30k registros/seg).
- Integración *full active directory*/LDAP para la autenticación, autorización y ajustes de correos electrónicos.
- Consultas arbitrarias en grandes conjuntos de datos.
- Dashboards a través de Google Visualizations.
- Alertas por correo electrónico y programación de reportes.
- Arquitectura plug-in para interfaz web.
- Arquitectura distribuida para clusters.
- Envía con la normalización de algunos registros de Cisco, Snort / Suricata, Bro, y Windows a través de Eventlog-to-Syslog o Snare.

[17] (Snorby, 2014)

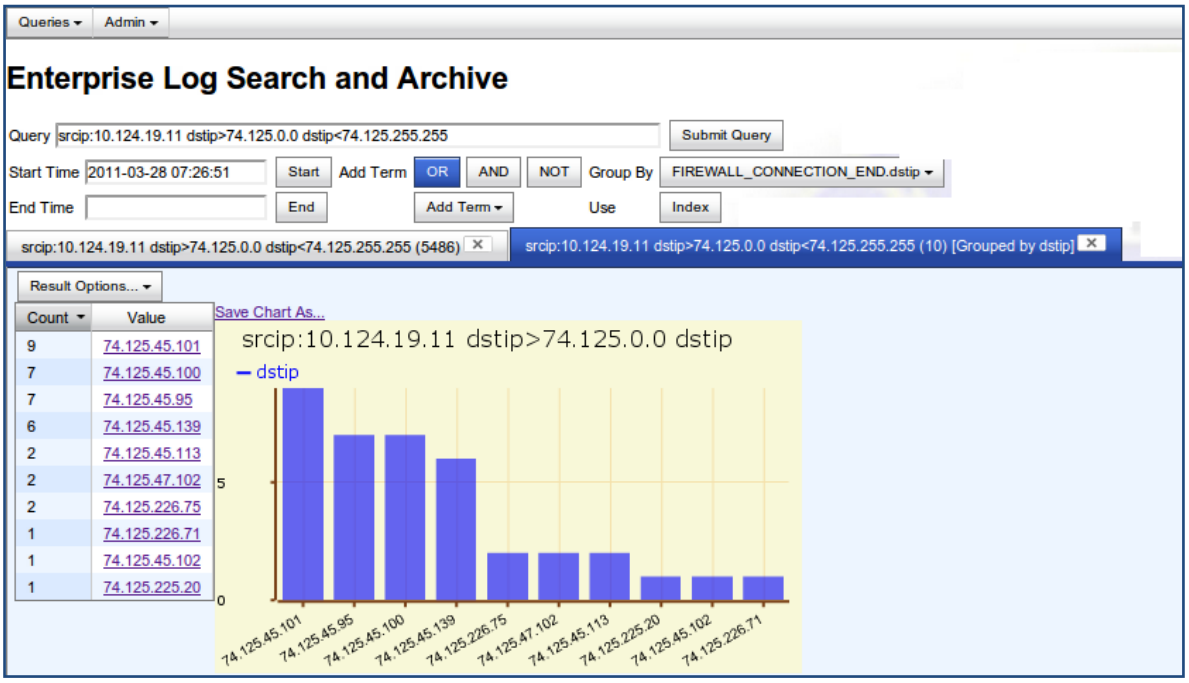

Figura 2.18. Tablas de ELSA.
Fuente: http://ossectools.blogspot.mx/2011/03/fighting-apt-with-open-source-software.html

Capítulo 3

Snort IDS (Intrusion Detection) y Snorby

CAPÍTULO 3

3.1 ¿QUÉ ES UN IDS?

Las siglas IDS hacen referencia a un sistema de detección de intrusos, es un mecanismo que está a la escucha de tráfico que viaja a través de la red, para poder detectar anomalías o comportamientos sospechosos, posibilitando con esto el riesgo de intrusión (Kioskea, 2013)

La detección de intrusos es el proceso del monitoreo de eventos que ocurren dentro de un sistema de cómputo o de una red, analizando las posibles violaciones o amenazas inminentes de incumplimiento de las políticas de la seguridad de cómputo.

Un sistema de detección de intrusos (IDS) es un software que automatiza el proceso de detección de intrusos. Las redes basadas en IDS son conocidas como NIDS, ésta monitorea el tráfico de un segmento de red en particular o dispositivos, analiza la actividad de la red y del protocolo de aplicación para identificar actividad sospechosa.[18]

Existe también otro tipo de IDS conocido como HIDS (Sistema de Detección de Intrusos en Host), este IDS se encuentra en un host en particular lo cual le permite cubrir varios sistemas operativos como Windows, Linux, Solaris, etc.

El HIDS analiza la información que esta almacenada en los registros del sistema, también captura paquetes de la red que entran y salen del host para poder verificar algún tipo de actividad sospechosa como denegación de servicios (DoS), puertas traseras, troyanos, ejecución de código malicioso o algún ataque de desbordamiento de búfer.[19]

Los sistemas de análisis de registros de seguridad conocidos como sistema de detección de intrusos basado en registros (LIDS) por sus siglas en ingles. El sistema de detección de intrusos para el análisis de registros es el proceso o técnica que se utiliza para detectar ataques sobre un entorno en específico, utilizando registros como la fuente primaria de información. Los LIDS son también

[18] (Gupta, 2012)
[19] (Kioskea, 2013)

utilizados para detectar el mal uso de las computadoras, violación de políticas o alguna otra forma de actividad inapropiada (Gupta, 2012)

Los NIDS y LIDS son necesarios para el monitoreo eficiente de seguridad en una organización. Ambas técnicas, la de detección basada en red y la que está basada en registros, se complementan una a la otra en la identificación y reporte de incidentes de seguridad (Gupta, 2012)

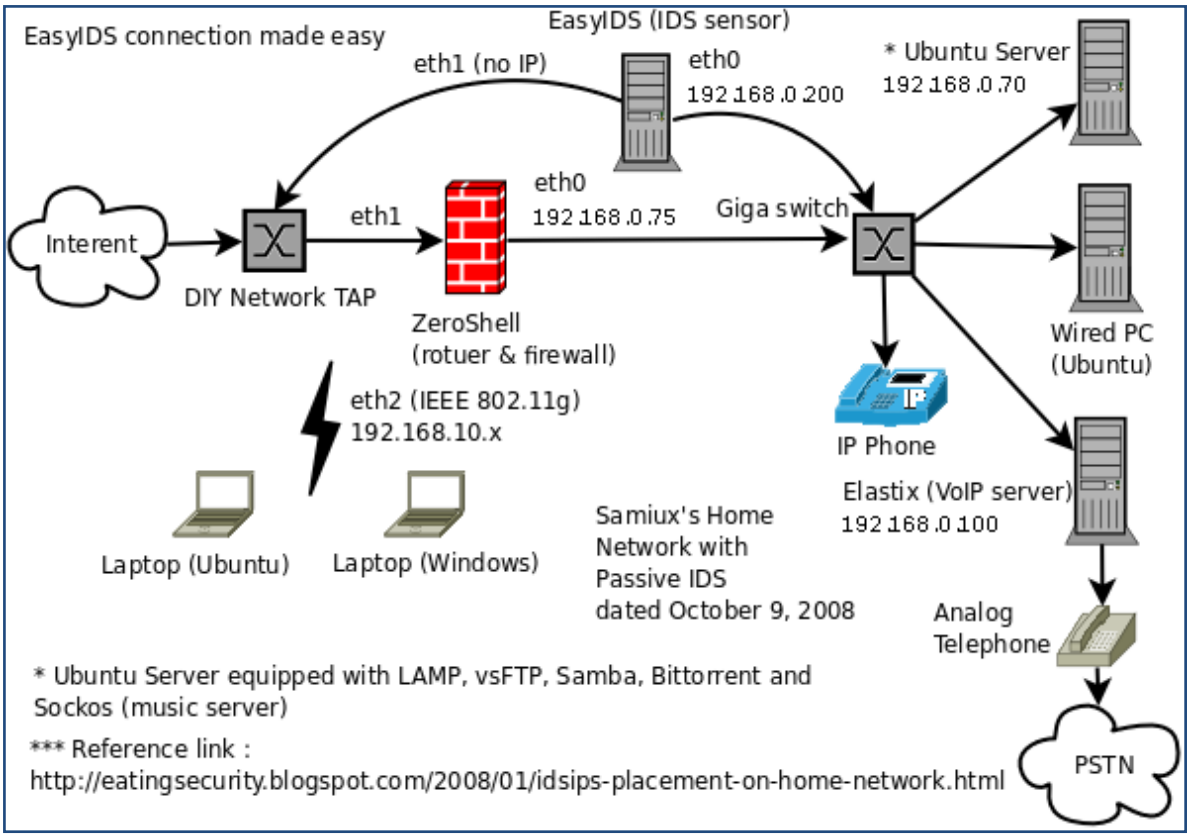

Figura 3.1. Estructura de un IDS.
Fuente: (Samiux, 2008)

Se muestra la estructura de un IDS (véase figura 3.1) dentro de una red.

Los métodos que utilizan los NIDS para notificar y bloquear intrusos son:

- Reconfiguración de dispositivos externos (firewalls): Es un comando que se envía por el NIDS hacia el firewall para reconfigurar dicho dispositivo y así bloquear la intrusión, la reconfiguración se da a través del envío de datos que explican la alerta que viene en el encabezado del paquete.

- Envío de notificaciones por correo electrónico: Envía un correo electrónico a uno o más administradores de red para la notificación de posibles intrusiones.
- Registro de ataques: Se almacena en un historial de eventos, detalles de las alertas generadas dentro de una base de datos, que incluye información como la fecha, dirección IP fuente, dirección IP destino, protocolos utilizados y carga útil.
- Almacenamiento de paquetes sospechosos: Almacena los paquetes capturados que ejecutaron la alerta.

La diferencia que existe entre un IDS y un IPS (Sistema de Prevención de Intrusos) es que el IDS reconoce las intrusiones y está a la escucha en la red. Mientras que el IPS es un sistema de prevención-protección de intrusiones, tiene la habilidad de bloquear de manera inmediata las intrusiones, sin importar el tipo de protocolo de trasporte usado y sin la necesidad de reconfigurar un dispositivo externo[20].

3.1.1 ¿QUÉ ES UN IPS?

Es una aplicación que controla el acceso hacia una red para poder proteger a los sistemas computacionales de ataques. Los IPS a diferencia de los IDS presentan una mejora en cuanto a las tecnologías de los firewall, dado que no hay necesidad de reconfigurar estos dispositivos para poder bloquear alguna intrusión, así como también tomar decisiones de control de acceso basado en el contenido del tráfico que viaja por la red.

El IPS funciona por medios de módulos, el IPS establece políticas de seguridad para proteger a los equipos o a la red en general de un ataque.

Los IPS se categorizan por la forma en que detectan actividad sospechosa en el tráfico de la red (véase figura 3.2)[21]

[20] (Kioskea, 2013)
[21] (Wikipedia, 2013)

- *Detección basada en firmas*: Es un sistema similar utilizado por los antivirus, es decir, tal como una huella digital, la firma identifica a un gusano, virus, anomalía de protocolo o tráfico malicioso en específico.
- *Detección basada en políticas*: El IPS necesita que las políticas sean especificadas de una manera clara.
- *Detección basada en anomalías*: El funcionamiento se basa en el patrón de comportamiento normal del tráfico.
- *Detección honeypot*: Funciona usando un equipo que está configurado para atraer a los atacantes sin necesidad de poner en riesgo al sistema real, esto es de ayuda para poder conocer el comportamiento de los ataques y las técnicas utilizadas para recrear los mismos ataques y así, poder crear mejor las políticas de seguridad.

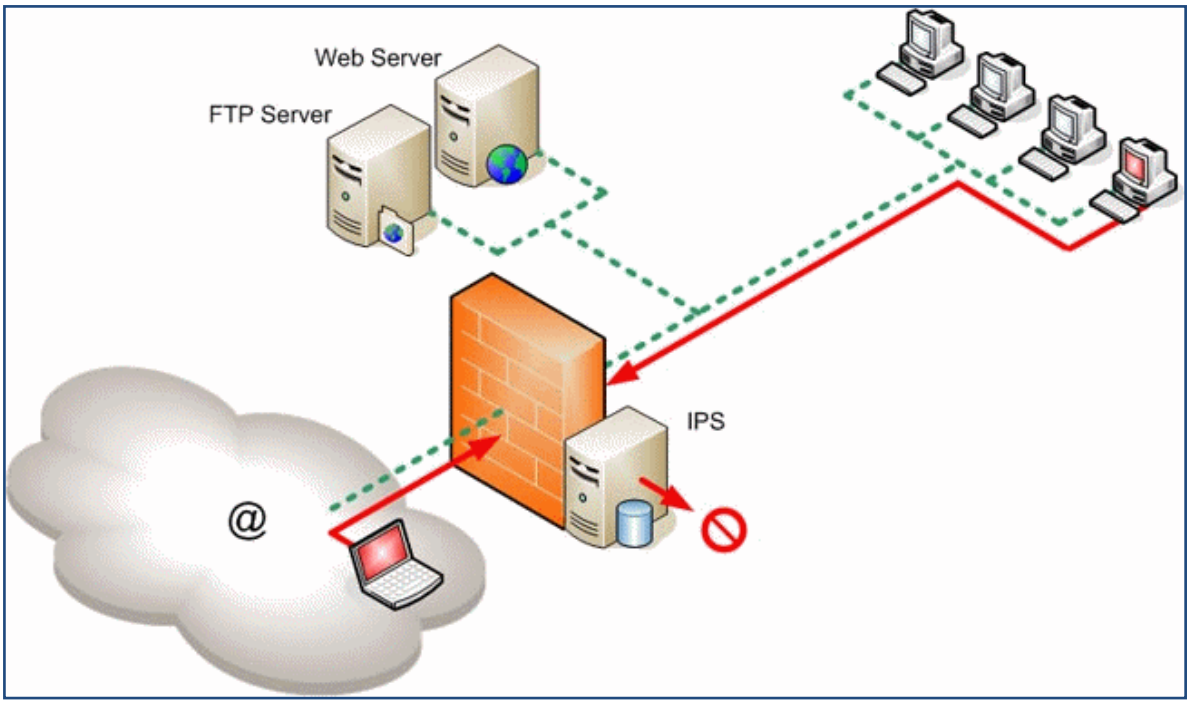

Figura 3.2. Estructura de un IPS.
Fuente: http://virusinformatico.net/

3.2 ¿QUÉ ES SNORT?

Snort (véase figura 3.3) es un sistema de detección y prevención de intrusos (IDS/IPS) de código abierto desarrollado por Sourcefire (Gupta, 2012). Es un software muy flexible, ofrece almacenamiento de bitácoras tanto en archivos de textos como de bases de datos como MySQL. Implementa un motor de detección de ataques y barrido de puertos lo que permite registrar, alertar y responder ante cualquier anomalía previamente definida.

Snort puede trabajar como sniffer lo que permite conocer en tiempo real lo que sucede en la red, registra los paquetes con la finalidad de poder analizarlos. Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, permite saber cuándo, dónde y cómo se produjo el ataque.

Snort está disponible bajo licencia GPL, gratuito y puede implementarse sobre Windows y UNIX/Linux. Cuenta con una gran cantidad de filtros predefinidos, actualizaciones ante casos de ataques, escaneo o vulnerabilidades que vayan siendo detectadas.

Figura 3.3. Logo de Snort.
Fuente: http://news.softpedia.com/newsImage/Snort-2-9-4-0-Provides-IPv6-Support-2.jpg/

Cuenta con una base de datos de ataques que está en constante actualización. Los usuarios pueden crear firmas basadas en características de ataques de red y mandarlas a una lista de correo de firmas de Snort, para que todos los usuarios de

Snort puedan utilizarlas y personalizarlas de acuerdo a las necesidades de la organización.[22]

Antes de continuar con la instalación y configuración de Snort, se debe conocer las posibles ubicaciones del IDS/IPS en la red. La ubicación se selecciona de acuerdo al tráfico que se quiere monitorear: paquetes de entrada, paquetes de salida, dentro del firewall, etc.

El IDS se debe colocar de manera que garantice la interoperabilidad y la correlación en la red, la interoperabilidad permite que el IDS/IPS pueda compartir u obtener información de otros sistemas como el firewall, routers y switches.

El IDS se pude colocar de las siguientes maneras:[23]

- *Delante del firewall*: De esta manera el IDS/IPS podrá comprobar todos los ataques producidos, aunque algunos o la mayoría no se concluyan, el firewall también bloquea los ataques.
- *Detrás del firewall*: Realiza el monitoreo del tráfico que entra en la red que no ha sido bloqueado por el firewall, los ataques que se detectan en ese punto son mucho más peligrosos.

Snort puede configurarse como un NIDS utilizando un puerto spanning. La configuración personalizada de Snort es creada por esta interfaz en el archivo que se encuentra en la siguiente dirección `/etc/nsm/HOSTNAME-INTERFACE1/Snort.conf`. Las variables de red, las bibliotecas cargadas dinámicamente y los preprocesadores son configurados para coincidir con el entorno personalizado en el archivo de configuración de Snort.

Las reglas personalizadas y la clasificación de las reglas son agregadas a `local.rules` y a `classifications.config` respectivamente a la ubicación `/etc/nsm/rules/`. Las reglas personalizadas para un sensor en específico son agregadas al respectivo sensor `/etc/nsm/HOSTNAME-INTERFACE1/rules/local.rules`.

Las clasificaciones personalizadas están definidas para el archivo de configuración `/etc/nsm/HOSTNAME-INTERFACE1/classifications.config`.

[22] (Torres, 2012)
[23] (Adminso, 2013)

Los datos del sensor son recolectados en el directorio `/nsm/sensor_data/HOSTNAME-NIC1`.

Las alertas de Snort están configuradas para la salida en el formato binario unified2. El archivo barnyard2 está configurado para analizar aquellas salidas de Snort dentro de la base de datos de Sguil y Snorby.[24]

3.2.1 FUNCIONAMIENTO DE SNORT

Snort puede funcionar de tres maneras, a continuación se explica cada uno (Torres, 2012)

- *Modo sniffer*: En este modo Snort va a monitorear en tiempo real toda la actividad que está en la red sobre la cual Snort está configurado.
- *Modo packet logger o registro de paquetes*: Aquí se almacenarán en un sistema de registros, toda la actividad de la red en que se ha configurado Snort para poder realizar un análisis de dichos registros.
- *Modo IDS*: Se monitorea toda la actividad de la red a través de un fichero de configuración, en donde se especifican las reglas y patrones a filtrar para el estudio de posibles ataques.

Ahora se explica acerca de la instalación de Snort que suele ser sencilla, los pasos que a continuación se mencionan son para la instalación sobre un sistema Linux.

Para descargarlo de manera directa se obtendrá de la siguiente manera:

```
apt-get http://www.snort.org/dl/snort-2.9.5.6.tar.gz
```

Una vez descargado el paquete se descomprime como sigue a continuación:

```
tar –xvfz Snort-2.9.5.6.tar.gz
```

Luego se cambia a la carpeta de snort-2.9.5.6

```
cd snort-2.9.5.6
```

Snort trabaja con una amplia variedad de bases de datos, la elección dependerá de lo que se quiera hacer y de la cantidad de tráfico con la que se quiere trabajar.
En este ejemplo se instalará MySQL como base de datos para Snort, se compila como se muestra a continuación:

```
./configure --with-mysql
make
make install
```

Para evitar posibles errores durante la compilación primero se debe de asegurar que se tengan todas las dependencias, aquí se mencionan algunas como `pcre.h, pcap.h, pcapbpf.h y mysql.h`, deben de estar en el directorio `/usr/include`. Una vez hecho *make* y *make install* se dan los últimos detalles antes de pasar a la configuración de la base de datos MySQL.
Los siguientes comandos sirven para crear los directorios necesarios para los archivos de configuración requeridos por los archivos de configuración, reglas y registros de Snort, para esto se debe de crear el directorio */etc/snort*.

```
mkdir /etc/snort/
mkdir /etc/snort/rules
mkdir /var/log/snort
```

Para poder acceder a las últimas reglas de Snort, se debe de estar registrado en la página, existen reglas que se comparten con la comunidad y se pueden adecuar a las necesidades de la organización o se puede optar por pagarlas, esta última se actualiza 30 días antes que las compartidas por la comunidad de manera gratuita.

[24] (Gupta, 2012)

De cualquiera de las maneras anteriores por las cuales se obtuvieron las reglas, se descomprimen en el directorio */etc/snort/rules*.
Ahora se crean los siguientes archivos snort.conf e icmp.rules.

```
# cat /etc/snort/snort.conf
include /etc/snort/rules/icmp.rules
# cat /etc/snort/rules/icmp.rules
alert icmp any any -> any any (msg:"ICMP Packet"; sid:477;
rev:3;)
```

Arriba se muestra una regla personalizada que alerta en caso de ver un paquete ICMP (ping)
A continuación se muestra la estructura de una regla en Snort en caso que se quieran hacer reglas personalizadas.

```
<Rule Actions> <Protocol> <Source IP Address> <Source Port>
<Direction Operator (->, <-)> <Destination IP Address>
<Destination> (rule options)
```

Las reglas de Snort son muy poderosas, flexibles y relativamente fáciles de escribir. Todas las reglas siguen un simple formato y define lo que Snort debería de monitorizar, como las cabeceras, los payloads o ambos. Las reglas de Snort están divididas en dos secciones lógicas, la cabecera de la regla y el cuerpo de la regla, como se observa en este otro ejemplo:

```
alert udp any any -> $central-log-server 514 (msg: "Windows
Anonymous Network Logon"; content:"Security, 540, "; nocase;
content: "anonymous"; nocase; reference:bugtrack, 540;
reference:url,http://www.url.com/securitylog/enciclopedia/eve
nt.aspx?eventid=540; classtype:attemped-user; priority:2;
sid:505401; rev:1;)
```

En este ejemplo, la primera parte del encabezado de la regla antes de "(" describe la regla para alertar ante cualquier evento que contenga tráfico UDP desde cualquier dirección IP, cualquier puerto al servidor, en este caso el puerto 514.

La segunda parte del cuerpo de la regla busca en la carga útil el contenido de "Security, 540," único en el inicio de sesión exitosa de la red de Windows y, a continuación el contenido de "anonymous" para inicio de sesión de usuario anónimo. Se asigna un id "505401", el nivel de revisión "1", la prioridad "2" y un mensaje de la regla "Windows Anonymous Network Logon" para identificar la regla.[25]

Snort ofrece varias opciones para la prevención/detección de intrusos. Los principales modos para la prevención de intrusos son el filtrado integrado, la cooperación con el firewall y el modo TCP-RST.

Cuando Snort trabaja en modo de filtro integrado, el tráfico va a pasar por él antes de que llegue a la red interna de la organización. Si el tráfico manda una alerta se desecharan los paquetes que activaron esa alerta.

La prevención de intrusiones puede impedir el acceso a los sistemas debido a falsos positivos o volver lenta la red en caso de que haya más tráfico del que el sensor de Snort es capaz de manejar.

Si se dispone de un firewall basado en iptables, se puede configurar Snort para modificar las reglas dinámicamente. La opción de iptables reduce el retardo del tráfico de entrada, en sí, el sistema será más lento en la respuesta a los ataques. Cada vez que el tráfico malicioso activa una alerta, Snort envía un comando al sistema que tiene iptables para que bloquee el ataque. La desventaja es que si no se configura correctamente, éste podría ser manipulado por el atacante permitiéndole lanzar un DoS hacia el sistema.

La configuración del IDS/IPS depende de los requisitos de seguridad de la organización en donde se implemente. Si se pretende un Snort como IPS, lo primero que debe de hacer es probar el servidor en modo IDS hasta que se haya

[25] (Gupta, 2012)

configurado de manera correcta y haber reducido el número de falsos positivos. Una vez hecho esto, ya se puede dejar Snort en modo de IPS.[26]
Ahora para ejecutar Snort desde la línea de comandos:

```
snort –c /etc/snort/snort.conf –l /var/log/snort/
```

Se debe introducir en la base de patrones de ataques que se quieren utilizar para detectar actividades sospechosas en la red. Una desventaja que podría existir es que demasiada seguridad podría volver vulnerable el sistema, es decir, si el usuario utiliza una gran cantidad de patrones para protegerse, creará una sobre carga de Snort lo cual dejará pasar los demás paquetes que no pueda analizar.
El motor de Snort se divide en los siguientes componentes[27]:

- *Decodificador de paquetes:* Toma los paquetes de diferentes tipos de interfaces de red, y prepara el paquete para ser pre procesado o enviado al motor de detección.
- *Preprocesador:* Los preprocesadores son componentes que utiliza Snort para arreglar, rearmar o modificar datos, antes de que el motor de detección realice una operación para ver si el paquete está siendo enviado por un intruso.
- *Motor de detección (comparación contra firmas):* El motor de detección es responsable de detectar la actividad de intrusión dentro de un paquete. Utiliza las reglas que han sido definidas con dicho propósito. Si un paquete coincide con una regla, la acción que viene dentro de la regla será aplicada a ese paquete.
- *Sistema de alerta*: Se encarga de iniciar sesión o generar una alerta, esto va a depender de lo que detecte el motor dentro del paquete. Los registros son almacenados en un archivo de texto con formato tcpdump.

[26] (Udenar, 2013)
[27] (Torres, 2012)

- *Plugins de salida*: Toman la salida del sistema de alerta y la almacenan en varios formatos o reaccionan ante el mismo, ejemplos de plugins de salida: MySQL, Postgres, syslog, XML.

3.3 TIPOS DE INTERFACES WEB PARA IDS

3.3.1 BASE

BASE es motor de búsqueda y análisis básico por sus siglas en ingles. Está sobre el código de Analysis Console for Intrusion Databases (ACID). Esta aplicación provee una interfaz web para consultar y analizar las alertas que vienen desde Snort (Johnson, 2014)

BASE es una interfaz web (véase figura 3.4) que realiza el análisis de intrusiones que Snort detecta sobre la red. Ésta utiliza un sistema de autenticación de usuarios y roles de base, por lo que el administrador de seguridad puede decidir qué y cuánta información puede ver cada usuario. También es muy sencillo de

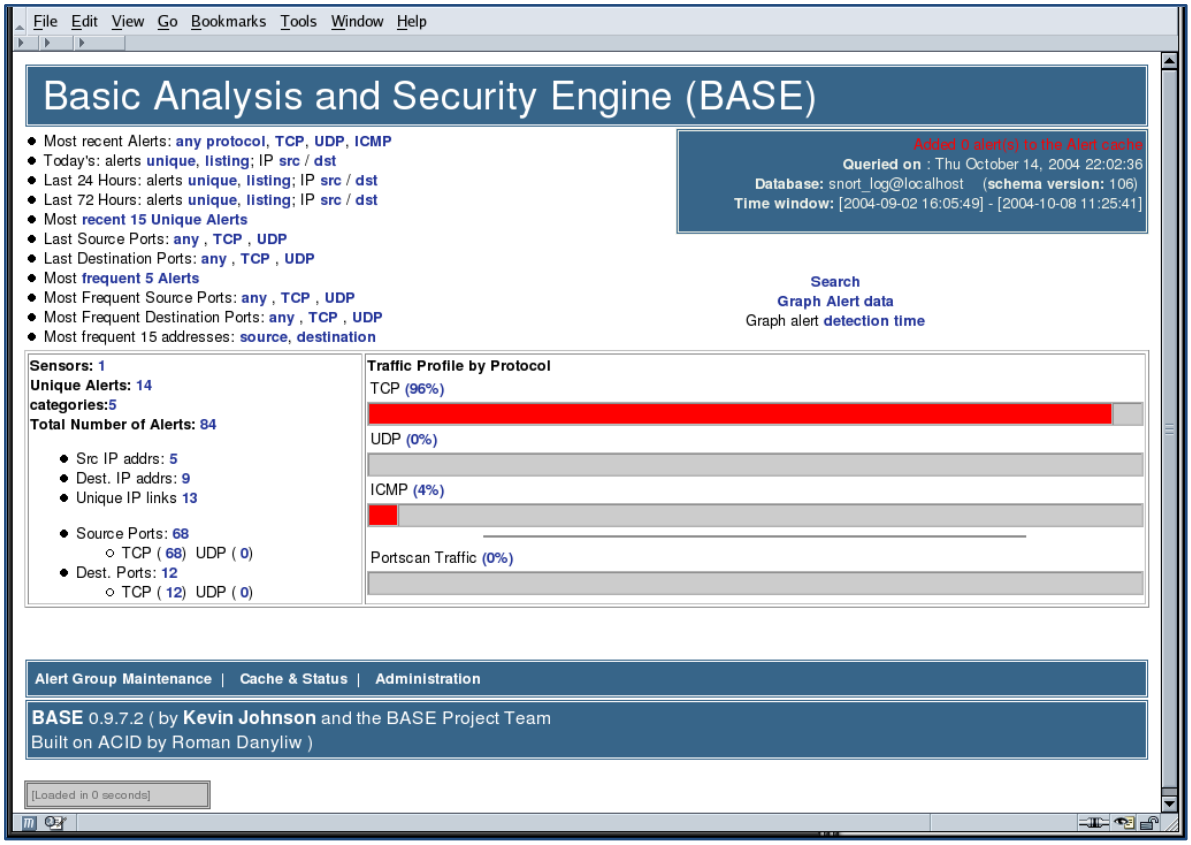

Figura 3.4. Pantalla de inicio de BASE.
Fuente: (Horn, 2010)

utilizar para las personas que no están familiarizadas con la edición de archivos ya que es un programa de configuración basada en la web.

BASE realiza búsquedas y procesos de los eventos registrados en la base de datos por las herramientas de monitorización de red como firewalls y programas IDS. Está escrito en PHP y muestra la información desde una base de datos con una interfaz web amigable para el usuario. Cuando es utilizado con Snort, BASE lee formatos de registros binarios como tcpdump y alertas de Snort. Una vez que los datos son registrados y procesados, BASE tiene la capacidad de mostrar la información de manera gráfica la capa 3 y la capa 4 del paquete (véase figura 3.5) También genera gráficas y estadísticas basadas en tiempo, sensores, firmas, protocolos, direcciones IP, puertos TCP/UDP o clasificaciones. La interfaz de búsqueda de BASE puede hacer consultas a la información que proviene del sensor, grupo de alertas, firmas, clasificación y detección en tiempo, así como los

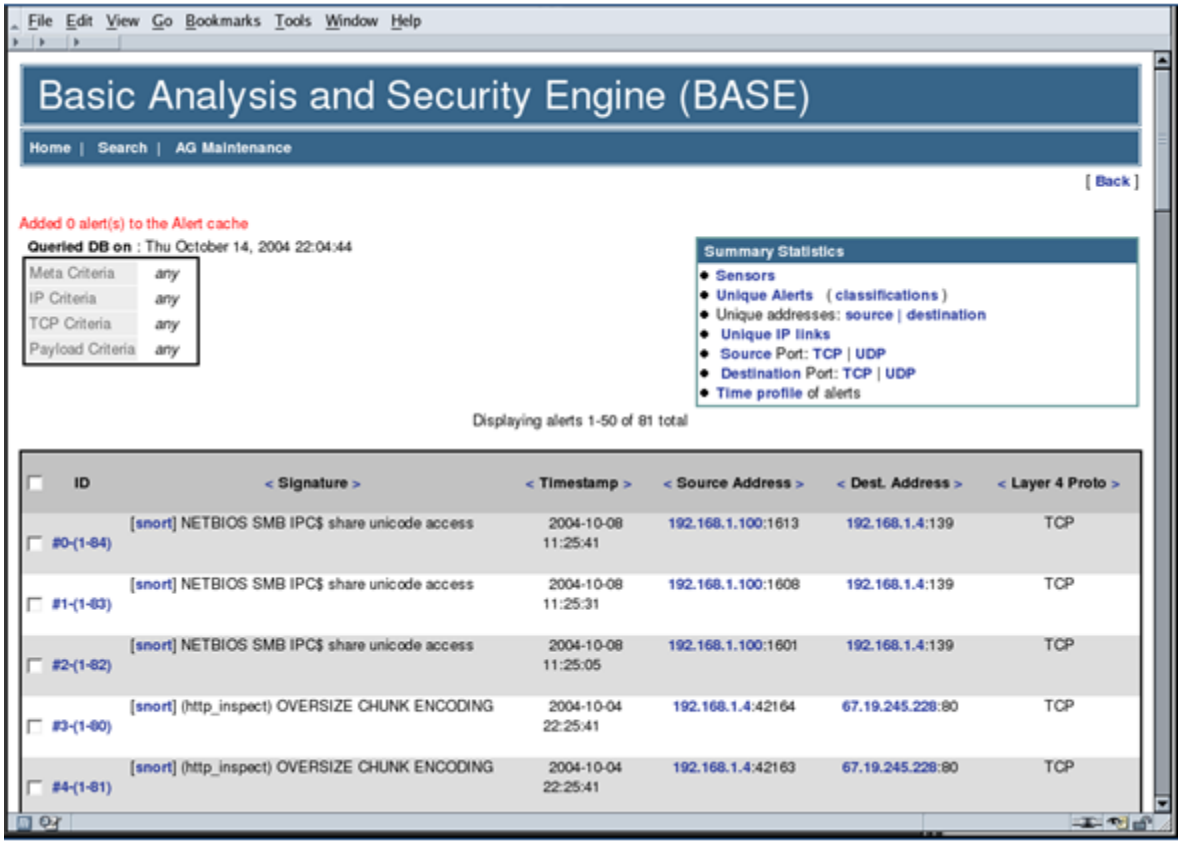

Figura 3.5. Registro de alertas detectadas por Snort.
Fuente: (Rich, 2005)

datos de los paquetes, como las direcciones de fuente/destino, puertos, payloads de los paquetes o banderas de los paquetes.[28]

BASE permite manejar las alertas de una manera fácil. El administrador puede categorizar los datos dentro de un grupo de alertas, eliminar falsos positivos o alertas atendidas anteriormente, exportar y archivar las alertas hacia una dirección de correo electrónico para administrar las notificaciones o su procesamiento.

Ahora para el funcionamiento de BASE primero se debe de instalar y configurar una base de datos, en este caso será MySQL, para almacenar las alertas de Snort. Además se necesitara Apache y Snort compilado con soporte para MySQL. También será necesario instalar PHP y los complementos de PHP. ADOdb es una biblioteca de PHP orientada a objetos, utilizada para la interfaz de la base de datos.

Después de realizar la configuración e instalar los complementos necesarios, se cuenta con un BASE funcional, el cual se podrá accesar desde *http://localhost/base*, estará listo para iniciar la GUI que permitirá la vista y manejo de las alertas.

Una vez iniciada la sesión, se muestra la página inicial que despliega un resumen de las actuales alertas registradas y enlaces a las gráficas.

Dependiendo de la lista, es posible explorar más abajo y ganar más detalle. Por ejemplo, en el enlace *Today's alerts: unique*, abre una nueva pantalla con un resumen de las alertas que se iniciaron la noche anterior. Un enlace con la etiqueta *Snort* situada a la izquierda de cada firma, cuando se da clic sobre ese enlace se re direcciona a la página de Snort para proporcionar más información de esa firma en particular.

El análisis a fondo de una dirección IP de origen y destino, aparecerá en un resumen que incluye el número de veces que aparece esa IP. También indica la primera y última vez que la IP fue registrada. Además, la página muestra el resumen que contiene los enlaces externos que proporcionan el DNS y servicios de consulta como Whois.

[28] (Rich, 2005)

El análisis de los enlaces de los puertos de fuente y destino, muestra un resumen de puertos, numero de ocurrencias, así como también la primera y última vez que fue visto. Cada puerto enlistado, tiene un enlace que re direcciona al SANS Internet Storm Center para conocer a detalle cada número de puerto.

BASE cuenta con una función que puede ser usada para realizar búsquedas rápidas, a través de la base de datos para ciertos criterios y presentarlos de manera ordenada como se muestra en la (véase figura 3.6)

Los criterios de búsqueda que son permitidos son los grupos de alertas, firmas y el tiempo de alerta. El resultado puede ser ordenado por marca de tiempo o *timestamp*, firma, IP fuente o IP destino; desafortunadamente, no hay una opción para usar una dirección IP como uno de los criterios.

Las gráficas pueden ser creadas desde datos de alerta o tiempo de detección de alertas. Los datos de alerta pueden ser graficados y trazados basándose en una variedad de opciones para crear reportes de fácil lectura.

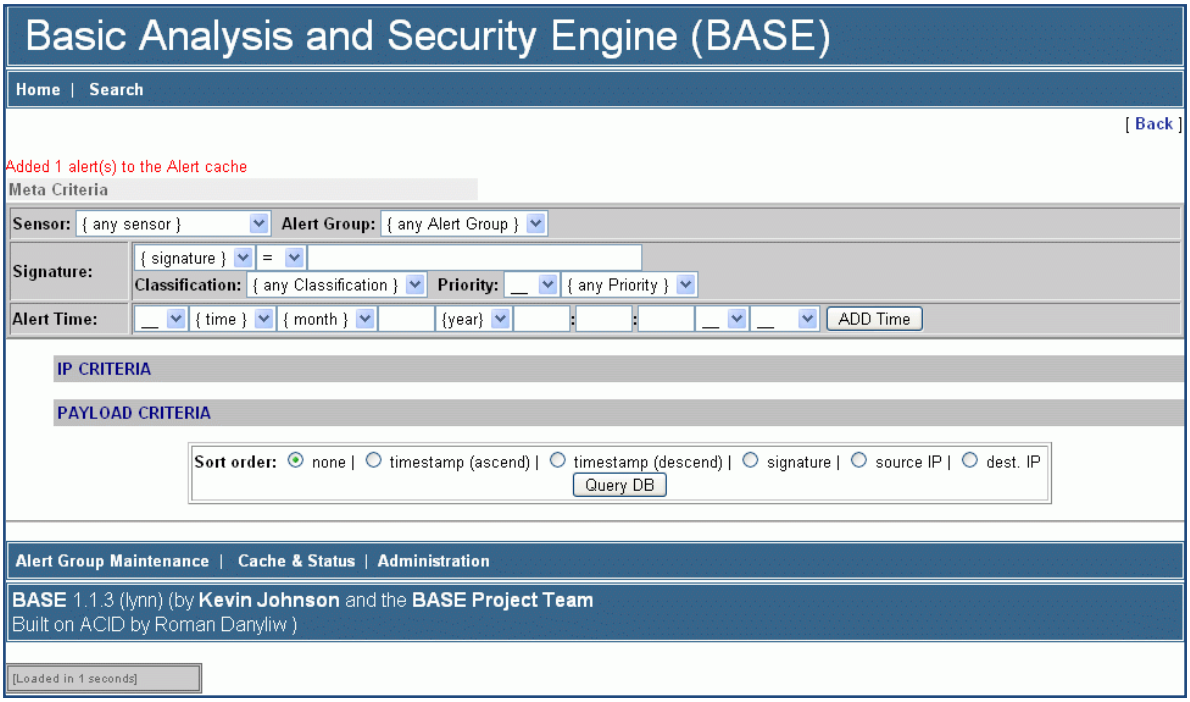

Figura 3.6. Función de búsqueda en BASE.
Fuente: (Rich, 2005)

Se muestra una gráfica de barras (con fines ilustrativos) basada en el tiempo de detección de alertas (véase figura 3.7), la cual puede ser utilizada para identificar periodos de intensa actividad.

Las gráficas y tablas le permiten al administrador del sistema visualizar con precisión los periodos de ataques.[29]

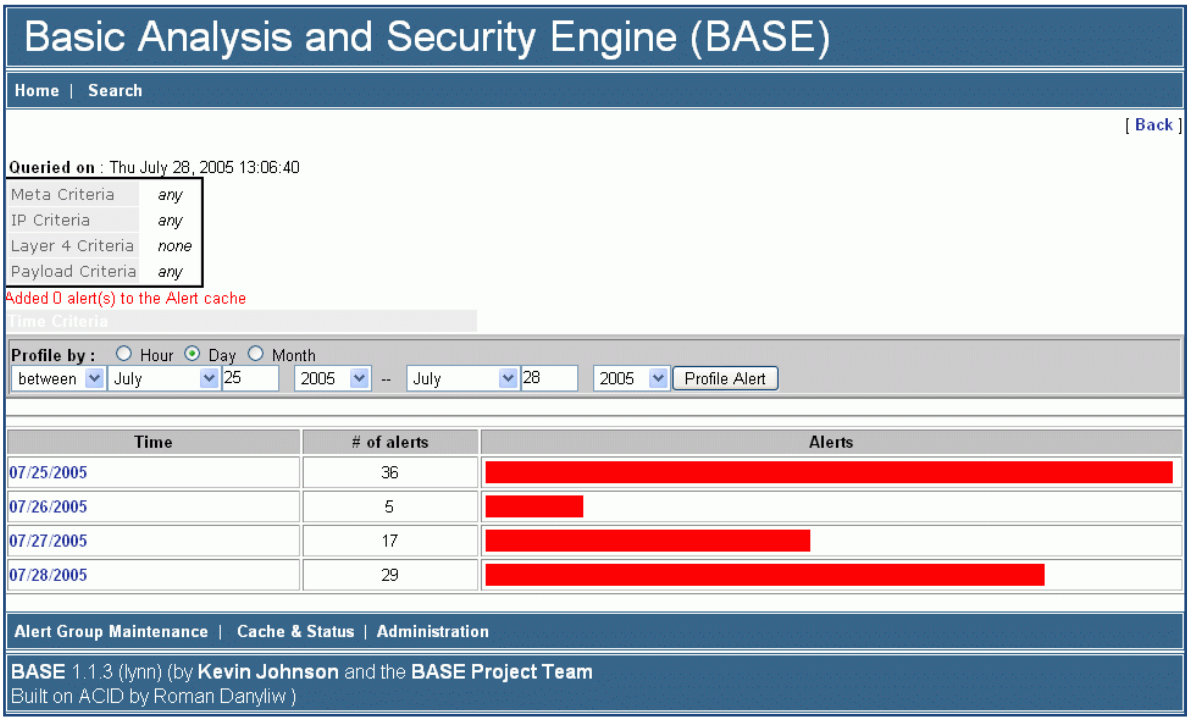

Figura 3.7. Gráfica de barras alertas vs. tiempo.
Fuente: (Rich, 2005)

[29] (Rich, 2005)

3.3.2 SNORBY

Snorby es un *front-end* para la gestión de alertas de Snort basado en sensores (véase figura 3.8) Puede integrarse con sistemas de detección de intrusos como Snort, Suricata y Sagan. El concepto fundamental detrás de Snorby es su simplicidad y poder.

Snorby proporciona una consola de fácil uso, que es configurable y funciona muy bien para cuando se realizan consultas y análisis detallados (Gupta, 2012)

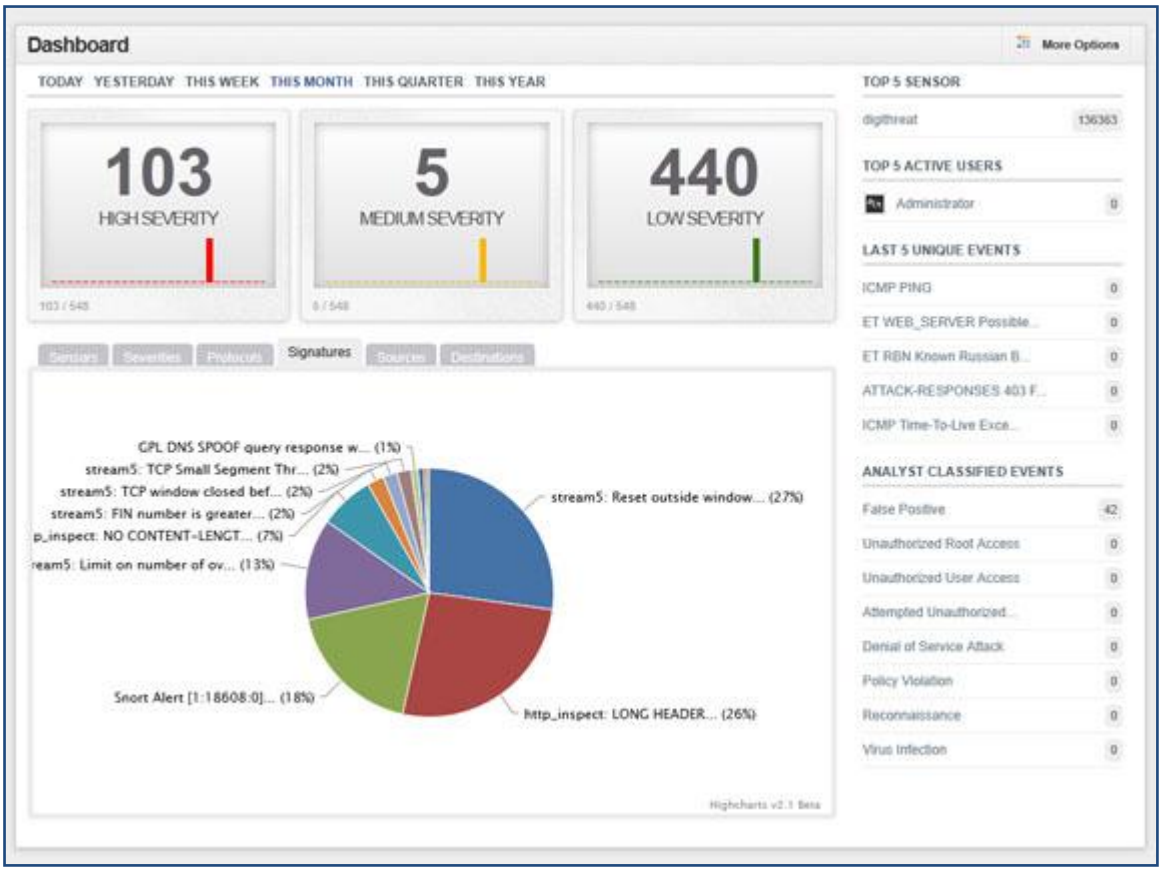

Figura 3.8. Dashboard de Snorby.
Fuente: (Snorby, 2014)

Algunas de las funciones de Snorby son:

- Dashboard con reportes de:
  - Numero de eventos de acuerdo al nivel de gravedad (alto, medio y bajo).
  - Conteo de eventos vs. tiempo por sensor.
  - Conteo de gravedad vs. tiempo.
  - Conteo de protocolos vs. tiempo.
  - Gráficas de distribución de firmas.
  - Gráficas de distribución fuente.
  - Gráficas de distribución destino.
- My queue: Permite eventos de distribución para una mayor investigación.
- Eventos: Línea de tiempo de eventos con detalles, incluyendo funciones de OpenFPC.
- Sensores: Lista de sensores.
- Búsquedas: Permite filtrar eventos por criterios.
- Administración: Administración de *backend* de la aplicación.

Existen 2 maneras de instalar Snorby:[30]

1.- Utilizar el instalador de Snorby llamado *Insta-Snorby*, es una máquina virtual con funciones de Snorby 2.2.6, Snort, Barnyard, OpneFPC y Pulled Pork que están configurados y listos para utilizarse.

2.- Instalar Snorby desde las fuentes, así como cada uno de sus componentes como Apache, MySQL, Oinkmaster, etc.

La arquitectura de Snorby (véase figura 3.9) puede ser considerada como una consola centralizada, recopilando registros desde IDS/IPS (Snort, Suricata, Sagan)

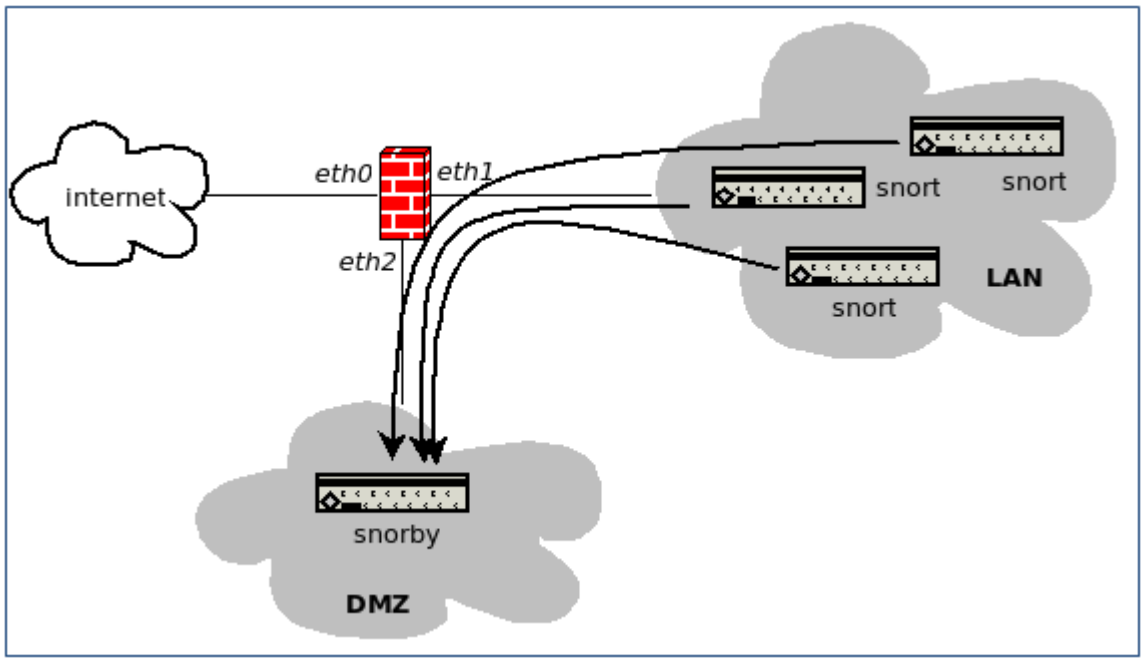

Figura 3.9. Arquitectura de Snorby.
Fuente: (Aldeid, 2013)

Ahora si se quiere enviar notificaciones de Snorby, se debe de configurar el archivo que está localizado en el directorio

`/usr/local/share/snorby/config/snorby_config.yml`

Deberá de tener los ajustes de dominio en la sección de producción que tiene que ser el nombre de dominio completo del servidor Snorby.

Lo siguiente es el archivo de configuración del correo electrónico `/usr/local/share/snorby/config/initializers/mail_config.rb` se necesita hacer lo mismo con los ajustes para el servidor de correos.

Entonces se reinicia el proceso de Snorby `delayed_job:`

```
$sudo pkill –f delayed_job
&sudo su www-data –c "cd /usr/local/share/snorby; bundle \ exec
rake snorby:update RAILS_ENV=production"
```

[30] (Aldeid, 2013)

Snorby trae los datos de monitoreo de seguridad de red con una magnifica suite[31]. Snorby es fácil de configurar; se pueden añadir niveles de gravedad personalizados o clasificaciones, se puede gestionar las notificaciones de correo electrónico e incluso ampliar la funcionalidad con otros productos, todo esto desde un menú muy intuitivo. Permite el intercambio de informes de datos como las comparaciones de la actividad del sensor o de las firmas más activas, con reportes diarios, semanales y mensuales. Las consultas son creadas sobre campos diferentes; estas consultas pueden también ser guardadas para futuros reportes.

[31] (Gupta, 2012)

Capítulo 4

Registro de incidentes con RTIR (Request Tracker for Incident Response)

CAPÍTULO 4

4.1 ¿PARA QUÉ SIRVE UN GESTOR DE INCIDENTES?

La gestión de incidencias tiene como objetivo principal resolver, de una manera más rápida y eficaz (OSIATIS, 2014), cualquier incidente que cause alguna interrupción en el servicio que se está prestando.

La gestión de incidencias no es lo mismo que una gestión de problemas, la diferencia radica en que la gestión de problemas no se preocupa de encontrar y analizar las causas subyacentes a un determinado incidente, sino exclusivamente a restaurar el servicio.[32]

Es importante también hacer referencia a las diferencias que hay en la gestión de incidencias con la gestión de peticiones, la gestión de peticiones se ocupa de las diversas solicitudes que los usuarios plantean para la mejora del servicio.

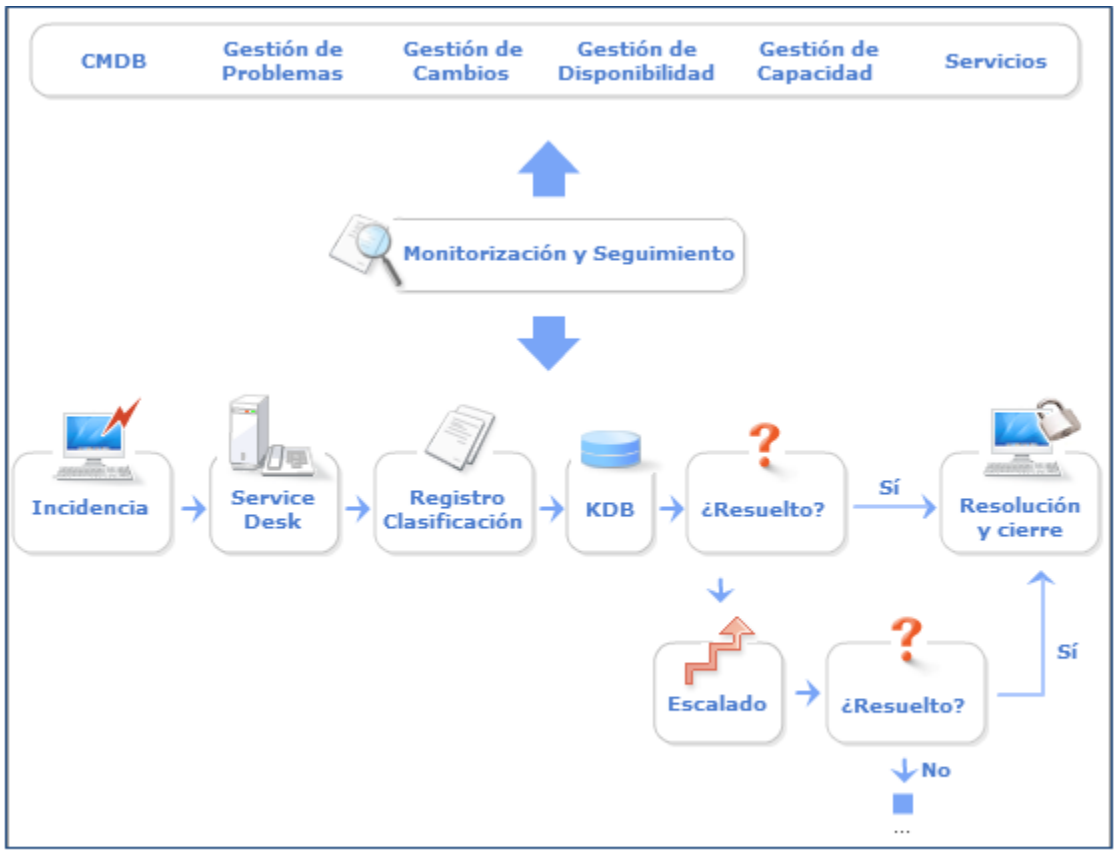

Figura 4.1. Ciclo de vida del manejo de un incidente.
Fuente: OSIATIS S.A

[32] (OSIATIS, 2014)

La incidencia será comunicada por el usuario o generada de manera automática por alguna aplicación. Se observa (véase figura 4.1) en ciclo de vida de un incidente.

En el *service desk*, es el área responsable de la gestión de incidencias.

El registro y clasificación, se crea el registro del incidente (prioridad= impacto*urgencia), se asigna tipo y personal de soporte.

En KDB se consulta en la base de conocimiento para ver si existe alguna solución a ese problema.

Después si se conoce un método de solución se asignaran los recursos necesarios, en caso contrario se escala la incidencia a un nivel superior de soporte.

Existen dos tipos de escalado en el proceso de resolución de incidencias, el escalado funcional que consiste en recurrir a técnicos de nivel superior y el escalado jerárquico en el cual entran en juego responsables de alto rango que están en la organización de TI.

En este segundo punto se vuelve a preguntar si ha sido resuelto, en caso afirmativo se asignan recursos necesarios para resolverlo, en caso negativo se vuelve a escalar la incidencia a un nivel superior de soporte.

La resolución y cierre, es cuando se ha resuelto el incidente satisfactoriamente, se registra el proceso en el sistema y si es de aplicación se registra en la base de conocimiento, si es necesario se genera un RFC (petición de cambio) a la gestión de cambios.

Monitorización y seguimiento, a partir de este punto todo proceso debe de ser controlado mediante la emisión de informes, actualización de la base de datos asociadas y se monitorean los niveles de servicio.

Debe de existir una relación muy estrecha entre la gestión de incidencias y otros procesos de TI con el objetivo de mejorar el servicio, conocer la capacidad y disponibilidad de la infraestructura de TI, así como también planificar y realizar los cambios necesarios para la optimización y desarrollo del servicio de TI.

Los objetivos principales para la gestión de incidentes son:[33]

- Detectar cualquier actividad fuera de lo normal en los servicio de TI.
- Registrar y clasificar actividad sospechosa en los servicio de TI.
- Asignar el personal encargado de restaurar el servicio.

El siguiente diagrama muestra (véase figura 4.2) cómo es el proceso de gestión de incidentes.

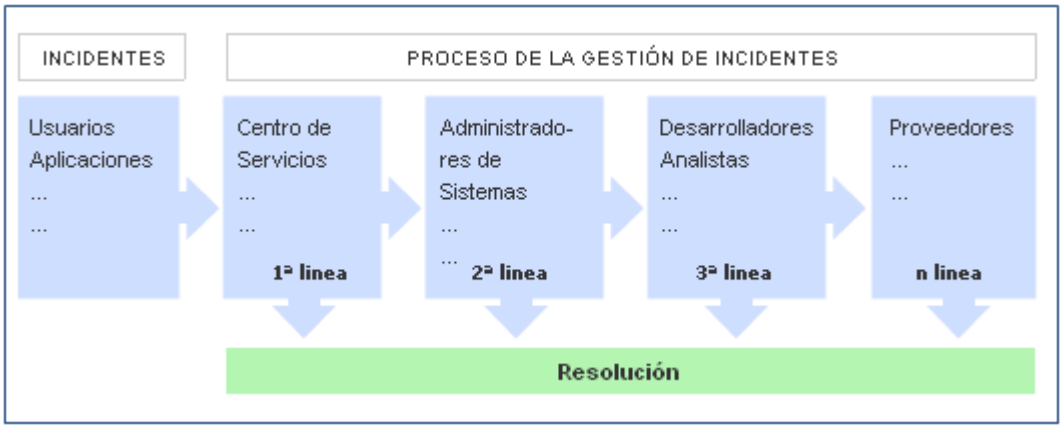

Figura 4.2. Proceso de la gestión de incidentes.
Fuente: (OSIATIS S. A.)

Una incidencia es: *"Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de la calidad del mismo".*[34]

Como en cualquier sistema estos pueden ser tanto beneficiosos como defectuosos, pero estas situaciones se deben al manejo que se le dé a la gestión de incidentes, a continuación se explican los beneficios de una correcta gestión de incidencias y la incorrecta gestión de incidencias.

[33] (OSIATIS, 2014)
[34] (ITIL, Fundamentos de Gestión, 2014)

Los beneficios de una correcta gestión de incidencias son:

- Mejorar la productividad de los usuarios.
- Cumplimiento de los niveles de servicio.
- Mayor control de los procesos y monitorización del servicio.
- Optimizar los recursos disponibles.
- Una base de datos de gestión de configuraciones más precisa, para registrar las incidencias en relación con elementos de configuración.

De otra manera si se realiza una incorrecta gestión de incidentes puede acarrear efectos negativos como:

- Disminuir el nivel y calidad del servicio.
- Demasiada gente o sin conocimiento, trabajando en la resolución de la incidencia.
- Perdida de información valiosa sobre las causas y efectos de las incidencias para posteriores reestructuraciones y evoluciones.
- Usuarios insatisfechos por la mala y/o lenta respuesta a los incidentes.

También pueden existir algunas dificultades al momento que se va a implementar la gestión de incidencias. No se siguen procedimientos acordados y se resuelven las incidencias sin registrarlas o que a veces se escalan innecesariamente, lo que conlleva la omisión de protocolos.

No existe un margen operativo que permita gestionar los niveles más altos de incidencias, por lo que éstas no se registran de manera adecuada e impiden la correcta operación de los protocolos de clasificación y escalado.

Frecuentemente existen múltiples incidencias concurrentes, por lo que es necesario determinar el nivel de prioridad para la resolución de las mismas.

La *priorización* se basa en el impacto y en la urgencia. Cuando se trata del impacto, determina la importancia de la incidencia dependiendo de cómo es que ésta afecta a los procesos de negocio y al número de usuarios afectados. La urgencia depende del tiempo máximo que tarde en que el cliente acepte para resolver la incidencia y el nivel de servicio acordado.

La prioridad del incidente puede cambiar durante su ciclo de vida, es decir, se pueden encontrar soluciones temporales que restauren los niveles de servicio y que permitan retrasar el cierre del incidente sin graves repercusiones.

Se muestra una gráfica (véase figura 4.3) que está en función de la urgencia e impacto del incidente.[35]

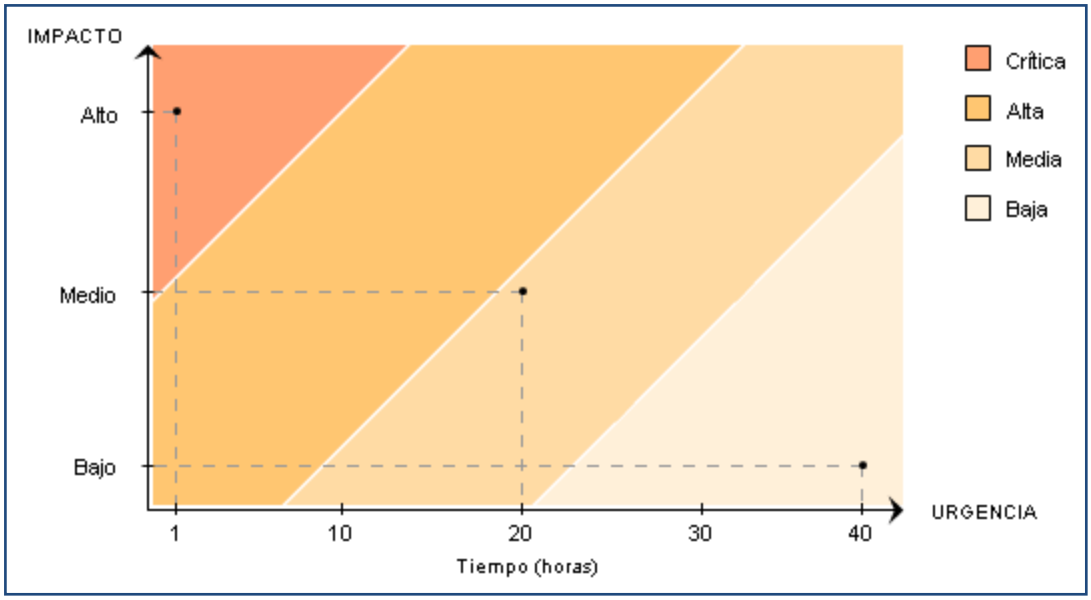

Figura 4.3. Diagrama de prioridades.
Fuente: OSIATIS S.A

Existen dos tipos de escalado, el *escalado funcional* que requiere del apoyo de un especialista de nivel alto para que resuelva el problema y el *escalado jerárquico* en el cual se debe acudir con un responsable que tenga un nivel alto de autoridad para que pueda tomar las decisiones que estén fuera de las atribuciones asignadas a ese nivel.

Se muestra de manera gráfica (véase figura 4.4) el proceso de escalado.[36]

[35] (ITIL, Conceptos Básicos, 2014)
[36] (ITIL, Escalado y Soporte, 2014)

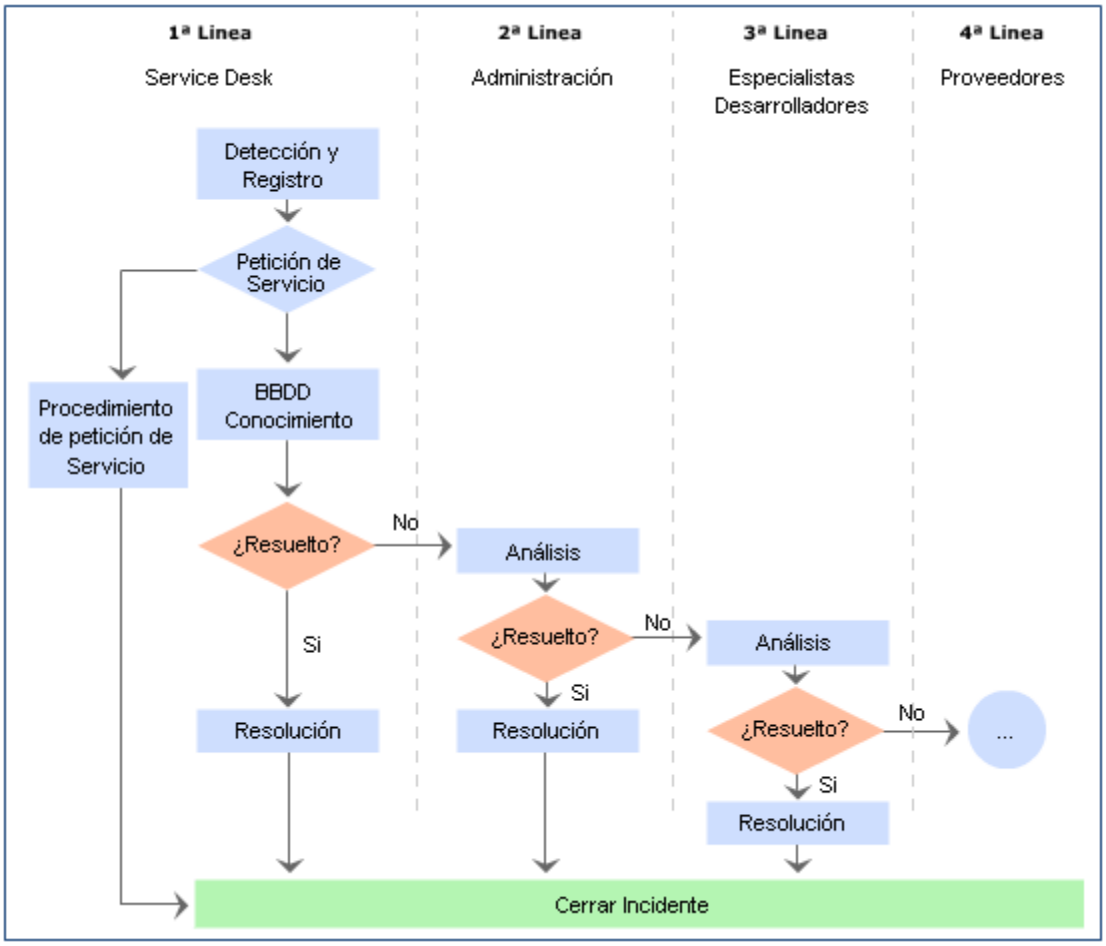

Figura 4.4. Proceso de escalado.
Fuente: OSIATIS S.A

Dentro del *registro y clasificación de incidentes* se sabe que las incidencias pueden provenir de varias fuentes como podrían ser los usuarios, el manejo de aplicaciones, el centro de servicio o soporte técnico.

El proceso de *registro* es una de las partes principales ya que si no se hace de manera inmediata se corre el riesgo de que aparezcan nuevas incidencias que demoren de manera indefinida el proceso. Durante este proceso se realizará la asignación de referencia, registro inicial, información de apoyo y notificación del incidente.

En la *asignación de referencia* se le asignará al incidente una referencia que le permitirá ser identificado en los procesos internos.

El *registro inicial* se va a introducir en la base de datos la información necesaria para el procesamiento del incidente (hora, descripción del incidente, sistemas afectados, etc.).

La *información de apoyo* se incluirá cualquier información relevante para la resolución del incidente.

Notificación del incidente, en los casos en que el incidente pueda afectar a otros usuarios, se les deberá notificar para que tengan conocimiento de que la incidencia puede afectar el flujo de trabajo.

La *clasificación* del incidente tiene como objetivo la recopilación de la información que pueda ser utilizada para la resolución del mismo, dentro de la clasificación se debe de categorizar, establecer el nivel de prioridad, asignar recursos, monitorización del estado y tiempo de respuesta.

El incidente se examina con la ayuda de una base de conocimiento para ver si se puede identificar con alguna incidencia que ya ha sido resuelta y aplicar el procedimiento asignado.

Puede ocurrir que el incidente este fuera de las posibilidades del centro de servicios éste lo redireccionara el incidente a un nivel superior para que ahí sea investigado por expertos.

La información que esta almacenada en la base de datos debe de actualizarse para que cualquier agente disponga de la información.[37]

Cuando el incidente se haya resuelto se debe de:

- Confirmar con los usuarios la solución exitosa del mismo.
- Incorpora el proceso de resolución a la base de conocimientos.
- Reclasificar el incidente si es necesario.
- Actualizar la información.
- Cierre del incidente.

4.2 Tipos de Gestores de Incidentes

4.2.1 RT (Request Tracker)

Es un sistema de seguimiento, es una manera de registrar las solicitudes que llegan por correo electrónico; para un seguimiento de respuestas y cambios en el estado de las solicitudes el cual es utilizado por cientos de organizaciones con la finalidad de dar seguimiento a fallos, servicio al cliente, procesos de flujo de trabajo, gestión de cambios, operaciones de red y servicios de orientación.

Las funciones de RT son:[38]

- Solicitudes o *tickets* pueden ser inicializados por correo electrónico; cada instancia de RT tendrá una dirección web y usualmente tendrá una o más direcciones de correo electrónico.
- Anexa y los cambios de estado se les dará seguimiento.
- RT cuenta con un sistema de privilegios lo cual le permite que diferentes usuarios puedan tener diferentes derechos para cambiar o asignar un *ticket*.

La lista de características de RT es extensa y por supuesto es completamente libre para su uso, las principales características de RT se enuncian a continuación.

La información crítica siempre estará disponible y toda en un solo lugar, la instalación de RT estará disponible en cualquier dispositivo que cuente con acceso a internet, por ejemplo una máquina de escritorio, laptop, tableta o teléfono. Como cualquier aplicación web no importa sobre que plataforma se esté trabajando ya sea Windows, Linux o Mac OS X.

No solo se puede utilizar RT sobre la web, sino también se puede tener interacción con RT vía correo electrónico. Se tendrá un correo sobre los cambios de RT, se puede responder desde la bandeja de entrada.

Para los más experimentados, RT cuenta con una API reset e incluso se puede comunicar con RT por medio de línea de comandos e integrarse con otros sistemas como ArcSIght, Nagios, Journix, MediaWiki, entre muchas otras.[39]

---

[37] (OSIATIS, 2014)
[38] (Chicago, 2012)
[39] (Practical, 2014)

Es completamente personalizable, es decir, se puede adecuar a las necesidades de la organización, RT permite categorizar los *tickets* y los proyectos, no hay un límite en la cantidad que pueda utilizar. Todo el flujo de trabajo y la lógica de negocio se pueden aplicar a RT utilizando poderosos "vales", ciclos de vida, campos personalizados, aprobaciones y extensiones que permiten pasar menos tiempo de mantenimiento de registros tediosos. RT cuenta con más de 15 idiomas, incluyendo Inglés, chino (tradicional y simplificado), español, francés, y muchos más.

Otras funciones con las que cuenta RT son:[40]

- Interfaz para optimización móvil (Android, iOS y WebOS).
- *Dashboards* y gráficas relacionales.
- Búsqueda de usuarios.
- Soporte PGP Seamless para cifrar, descifrar, firmar y verificar el correo electrónico que sale y entra.
- S/MIME, integración equivalente al soporte PGP.
- Edición de texto enriquecido para dar formato de manera más fácil a la correspondencia.
- Seguimiento y presentación de informes, incluyendo el apoyo a los acuerdos del nivel de servicio.
- Construcción de gráficas que resumen la actividad por el tiempo y otros campos.
- Integración con usuarios existentes en el sistema.

Se muestra la página de inicio de RT (véase figura 4.5)

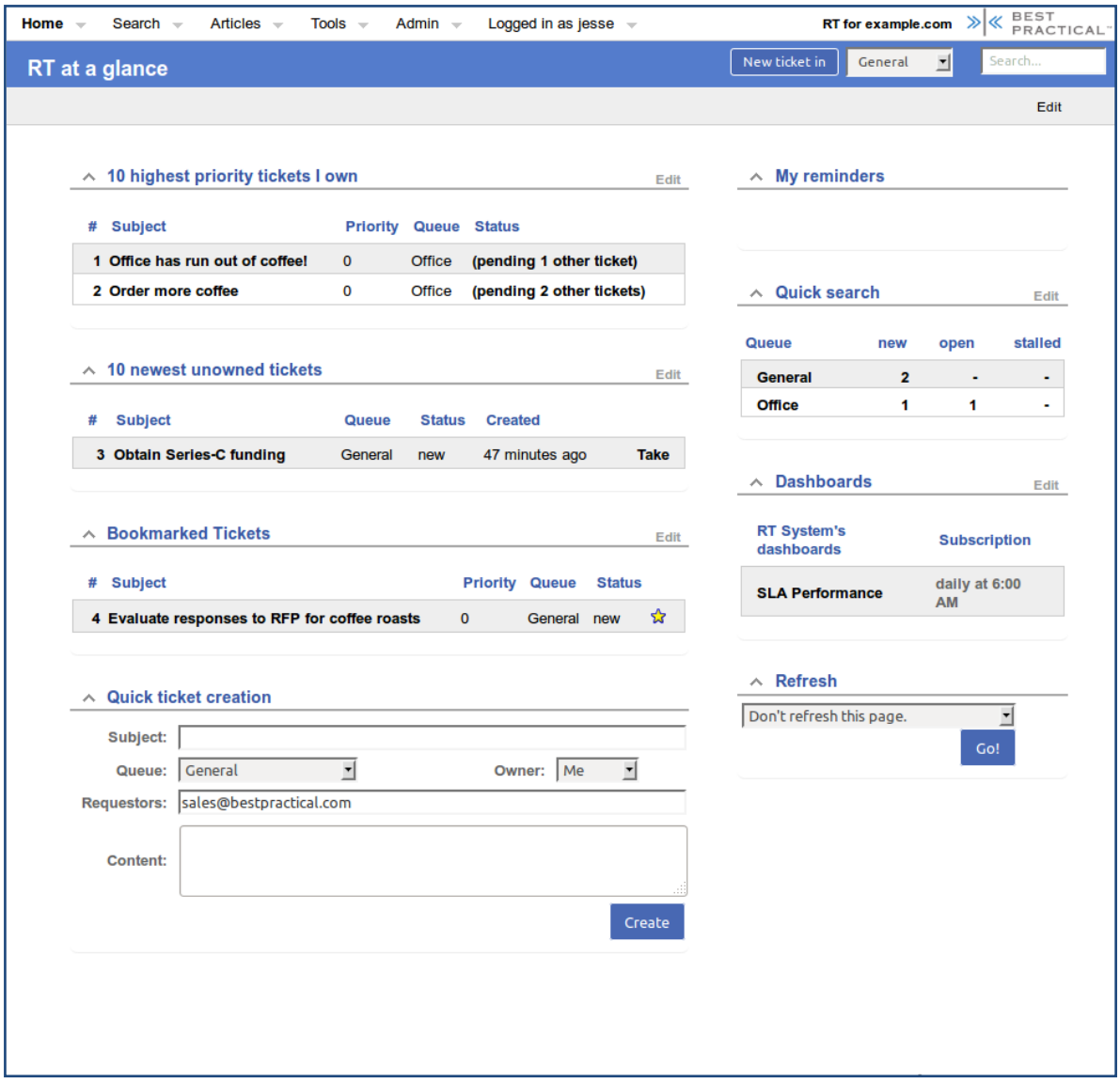

Figura 4.5. Página de inicio de RT.
Fuente: Best Practical Solutions LLC

[40] (Practical, 2014)

4.2.2 RTIR (Request Tracker for Incident Response)

Es un sistema que maneja incidentes de código abierto orientado para equipos de seguridad informática. Se trabaja con decenas de equipos de CERT y CSIRT alrededor del mundo ayudando al manejo del incremento en el volumen de reportes de incidentes. RTIR está construido sobre las funciones de RT.

JANET-CERT es un equipo de seguridad informática y respuesta a incidentes, ha venido trabajando con Best Practical para crear una versión de Request Tracker específicamente diseñado para trabajar la respuesta a incidentes (CSIRT, 2014)

Un flujo de trabajo se inicia con informes de incidentes entrantes y su vinculación con dicho incidente que ya existe o crear uno nuevo. Cada incidente está diseñado para mantener el seguimiento de cualquier cosa que se necesite conocer para resolver el problema. Desde un incidente, es fácil poner en práctica investigaciones para trabajar con la policía, proveedores de red u otras organizaciones (Response, 2014)

Se puede configurar bloques para hacer un seguimiento de lo que se ha hecho para mitigar el problema. Con código abierto, una API y una comunidad de usuarios, es fácil de integrar RTIR en un sistema existente y en un flujo de trabajo.

RTIR es una interfaz de usuario personalizada la cual se centra sobre lo alto de Request Tracker, un popular sistema de *tickets*. Todos los días el uso de RTIR es a través de una interfaz web y no requiere de un software adicional para ser instalado sobre la máquina del usuario (véase figura 4.6)

Antes de esto un miembro del equipo puede accesar a la interfaz de RTIR, necesitaran iniciar sesión al sistema con su cuenta de usuario y contraseña. RTIR se usa para tratar artículos usando cualquier cuenta como propiedad del usuario correspondiente, así como los atributos.

Algunas de las características de RTIR es que está diseñado específicamente para la respuesta a incidentes, RTIR automáticamente crea cuatro puntos RT para el seguimiento de incidentes (Response, 2014)

- Reporte de incidentes: Los nuevos informes tienen una fecha de vencimiento establecida y muestran una dashboard de RTIR.
- Incidentes: Los reportes de incidentes validos son puestos dentro de nuevos incidentes o enlazados a algunos que ya existen con un solo clic. Si se reciben múltiples reportes acerca del mismo problema, se pueden enlazar al mismo incidente para mantenerlos juntos y reducir la duplicación.
- Bloques: El seguimiento de las barreras configuradas en respuesta a un incidente para no dejarlos olvidados.
- Investigación: Toda la información relevante del incidente se incluye de manera automática cuando se inicia una nueva investigación.

RTIR utiliza el soporte de direcciones IP de RT para IPv4 e IPv6, así como también la indexación de texto completo, autocompletado de direcciones de correo electrónico, un editor de tema en línea y soporte continuo para encriptación PGP de un correo electrónico.

RTIR permite más control sobre la organización de *tickets*. Se puede compartir la investigación o bloques a través de múltiples incidentes o bloquear la creación de una investigación para requerir un incidente.

La integración de RTIR a una red existente y a las aplicaciones de seguridad con RT es simple y puede ahorrar tiempo. Ya se había construido una integración con ArcSight, Nagios y otro software.

Piezas relevantes de texto como las direcciones IP, nombres de dominio y URLs son enlazadas de manera automática a un resultado de whois, traceroute y a otros incidentes que contienen esas direcciones. En el contexto de un incidente, las direcciones de correo con un clic lanzan una investigación dentro de la parte nombrada.

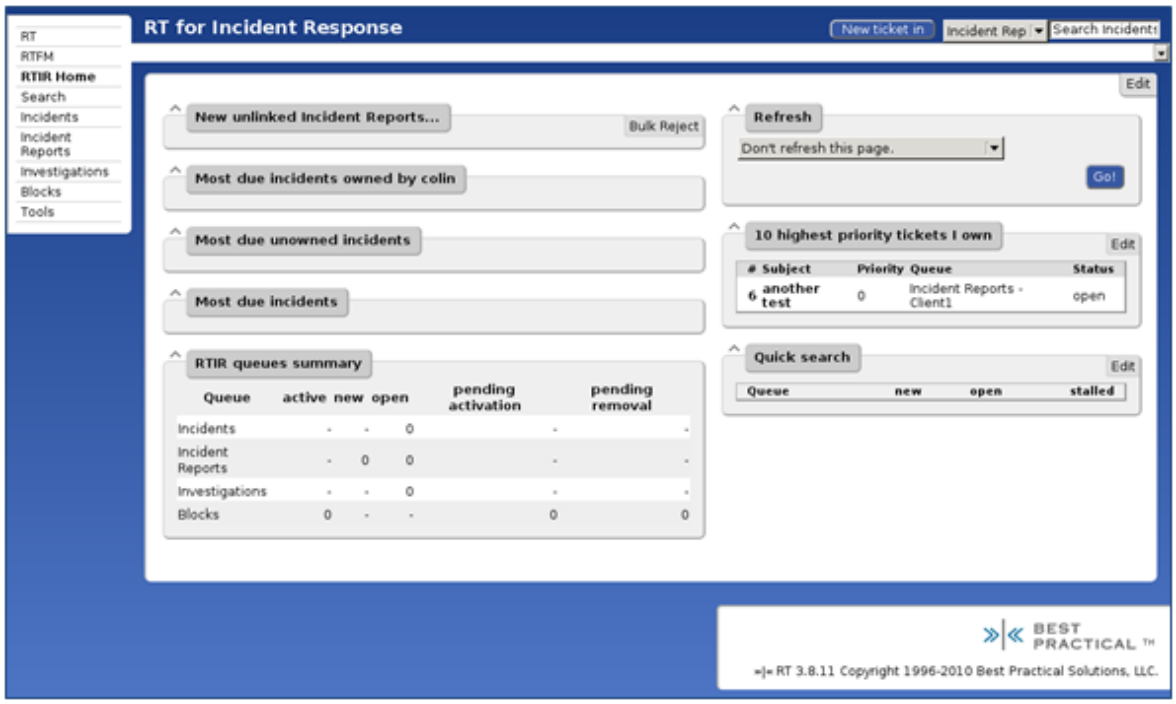

Figura 4.6. Página de inicio de RTIR.
Fuente: Best Practical Solutions LLC

Cuando se le da a RTIR una lista de IPs o de direcciones de correo puede crear automáticamente nuevos incidentes y enlazar investigaciones, y enviar una plantilla de mensajes para el usuario o administrador responsable.[41]

Las IPs se convierten en direcciones a través de las búsquedas whois a un servidor en específico.

La manera en que se generan los reportes es fácil, puede ser generado en archivos de texto, HTML o informes de hojas de cálculo, acerca del número de incidentes, su tipo y su resolución para cualquier periodo de tiempo arbitrario.

4.2.3 AIRT (Application for Incident Response Teams)

Es una aplicación basada en web que ha sido diseñada y desarrollada para soportar el día a día las operaciones de equipos de respuesta a incidentes de seguridad informática. La aplicación soporta procesamiento automatizado de reporte de incidentes y facilita la coordinación de múltiples incidentes para un centro de operaciones de seguridad.

El objetivo de AIRT (véase figura 4.7) son los grupos de respuesta a incidentes los cuales proveen apoyo a los usuarios finales. Está completamente desarrollado en PHP4 sobre una base de datos Postgresql.

AIRT es capaz de interactuar con cualquier IODEF (Incident Object Description Exchange Format). La base de usuarios de AIRT se compone de equipos de respuesta a incidentes de medio y gran tamaño, quienes reportan incrementos significantes en la productividad, cooperación más fácil con los miembros del equipo, y mejorando el seguimiento de incidentes durante el incremento de la carga de trabajo (McRee, 2009)

Los filtros de importancia son agregados regularmente lo cual permite el procesamiento automático de reportes generados por computadora, y los errores son solucionados con prontitud cuando son descubiertos o reportados.

Algunas de las características de AIRT son:

- Consola de manejo de incidentes.
- Rangos de direcciones (VLAN, redes)
- Tipos de incidentes, estados y estatutos.
- Plantillas de correo electrónico con PGP y GnuPGP.
- Ejecución de comandos asíncronos.

Figura 4.7. Página de inicio de AIRT.
Fuente: (McRee, 2009)

[41] (Practical, Request Tracker for Incident Response, 2014)

Capítulo 5

Aplicación

CAPÍTULO 5

5.1 BÚSQUEDA DE NOTICIAS POR MEDIO DE PALABRAS CLAVES

En esta última parte de la investigación se muestra de manera gráfica la aplicación de cada uno de estos módulos, se inicia con el motor de búsqueda de noticias, se explica paso a paso como es que se realiza la búsqueda de dichas noticias de interés.

Se muestra la caja de búsqueda (véase figura 5.1) junto con los botones de número de búsquedas a realizar y el de *search*.

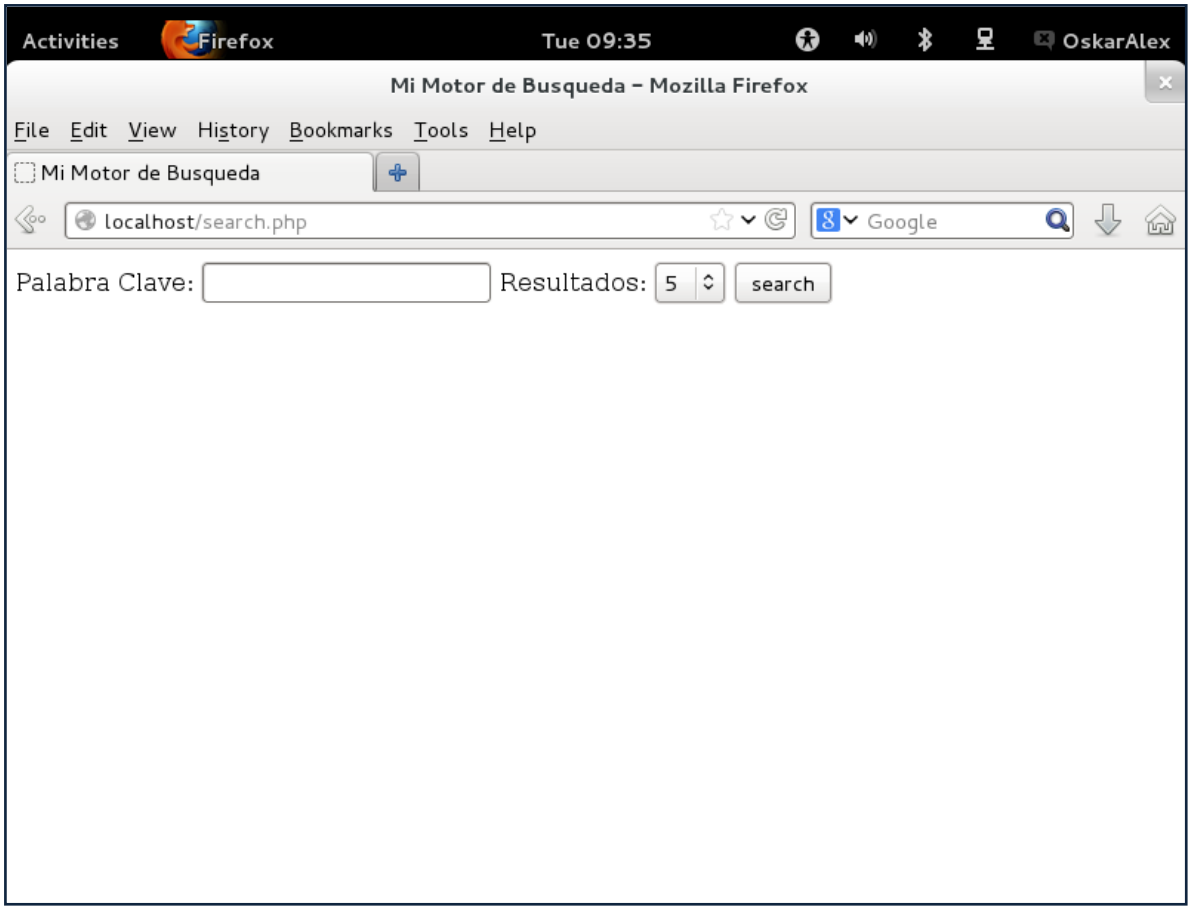

Figura 5.1. Página de inicio de buscador de noticias.
Fuente: (Firefox, 2014)

Una vez que se introduce la palabra que se desea buscar, muestra las páginas en la cuales coincide esa palabra, como se muestra (véase figura 5.2)

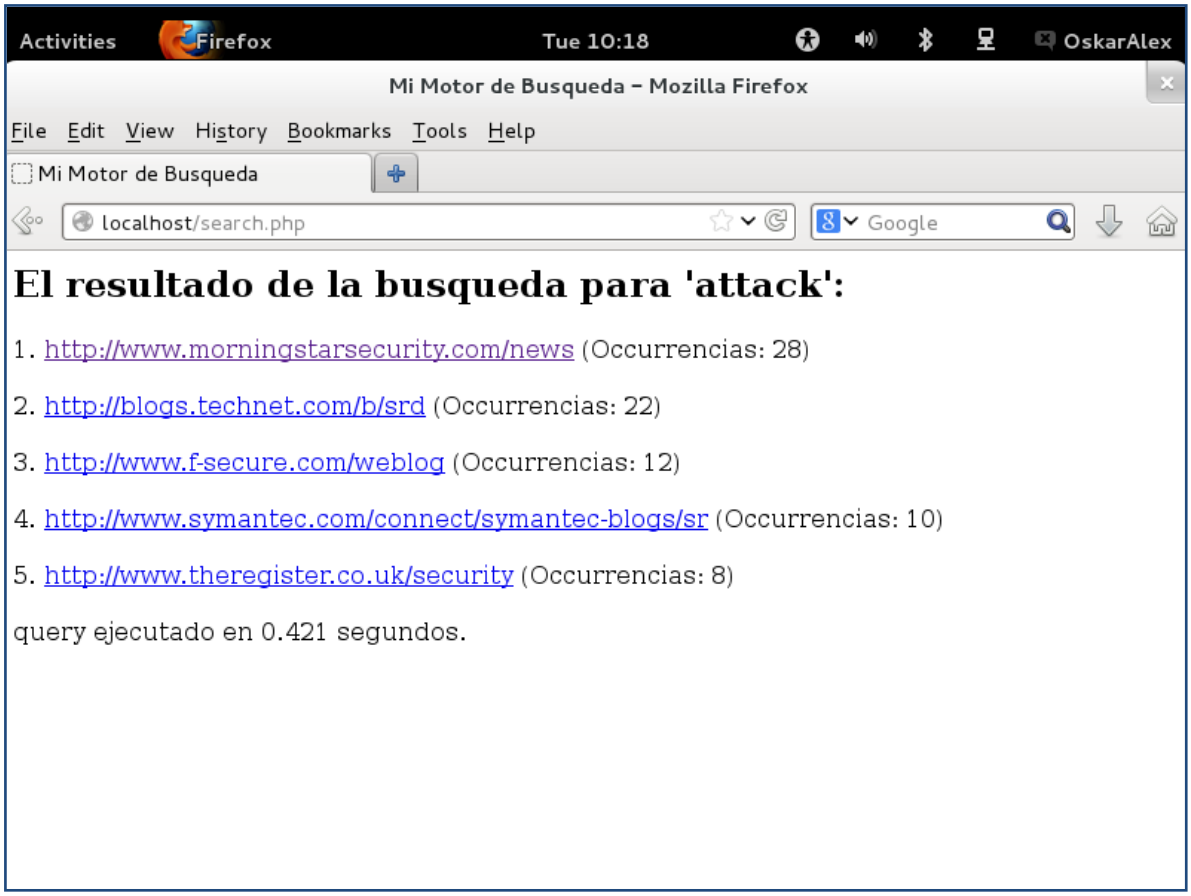

Figura 5.2. Resultados de la búsqueda de la palabra "attack".
Fuente: (Firefox, 2014)

Como se puede ver, arrojo las cinco búsquedas que se seleccionaron en la página de inicio, también muestra el número de veces que aparece la palabra *attack* en cada resultado. Se muestran las tablas (véase figura 5.3) en MySQL donde están almacenadas las URLs.

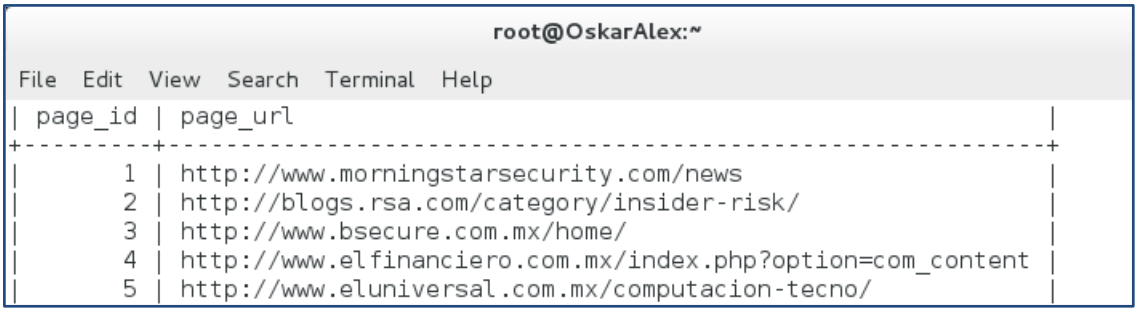

Figura 5.3. URLs que están dentro de la tabla page.
Fuente: (MySQL, 2014)

Las palabras que va a buscar son palabras que sean de interés para el área de seguridad informática en general como México, attack, anonymous, entre otras.
También se puede crear un canal RSS (Really Simple Syndication), este medio permite conocer noticias que nos interesen de una manera más rápida, se muestra un enlace (véase figura 5.4) que complementa al buscador de noticias utilizando el servicio de RSS.

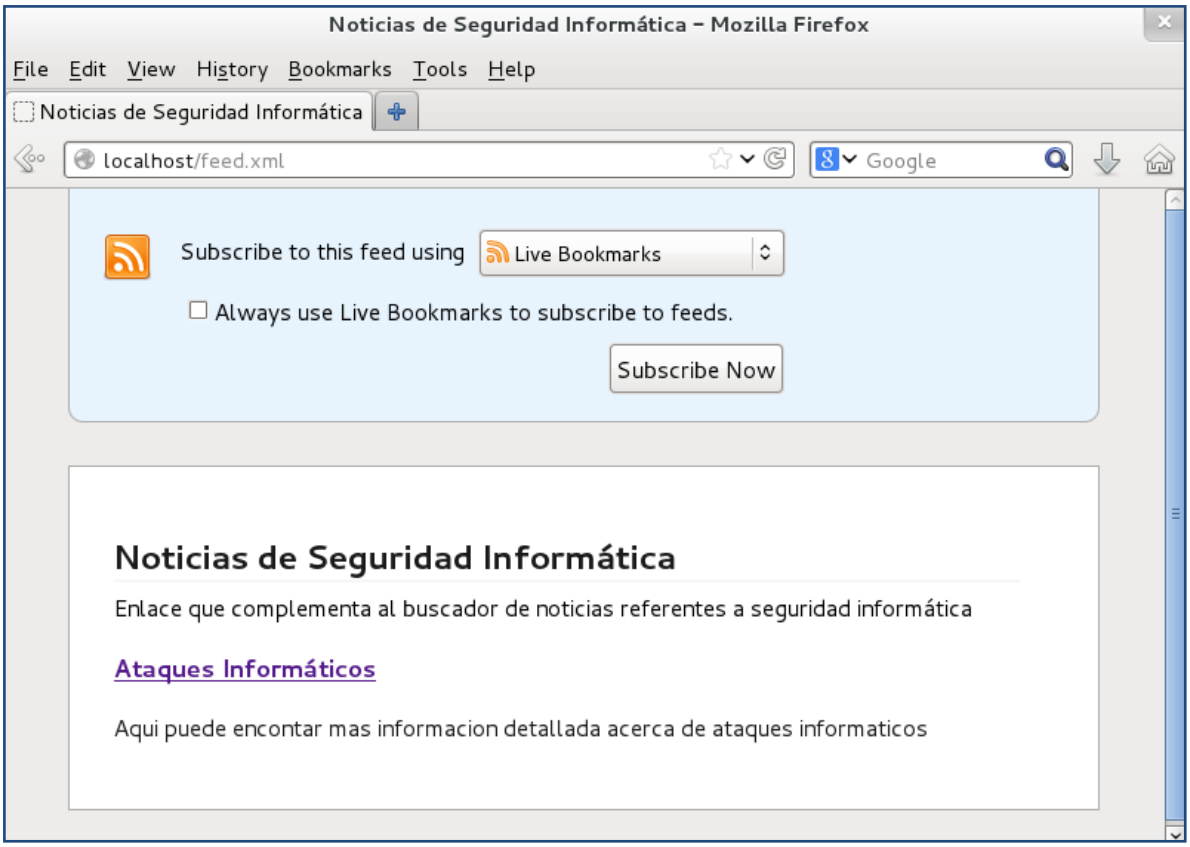

Figura 5.4. Servicio RSS.
Fuente: (Firefox, 2014)

Este tipo de servicio es muy eficiente porque se actualiza siempre la información con lo más relevante, RSS sirve para enumerar artículos o páginas dentro de un sitio, en un formato que pueden entender programas denominados lectores RSS o agregadores. Es un método sencillo, creado para compartir información en la red.

Es un sistema automatizado de envío de noticias en internet que permite a los suscriptores, estar actualizado con la información que publica regularmente el sitio web que les interesa.

5.2 DEMOSTRACIÓN DE ENVÍO DE PING A UN GRUPO DE IP EN PING TESTER

A continuación se muestra (véase figura 5.5), cómo hacer ping a un grupo de IPs así como también programar las veces en que se debe de enviar el ping, es una herramienta muy útil cuando se trata de conocer si los dispositivos están disponibles o no, dentro de la red. Ver figura siguiente:

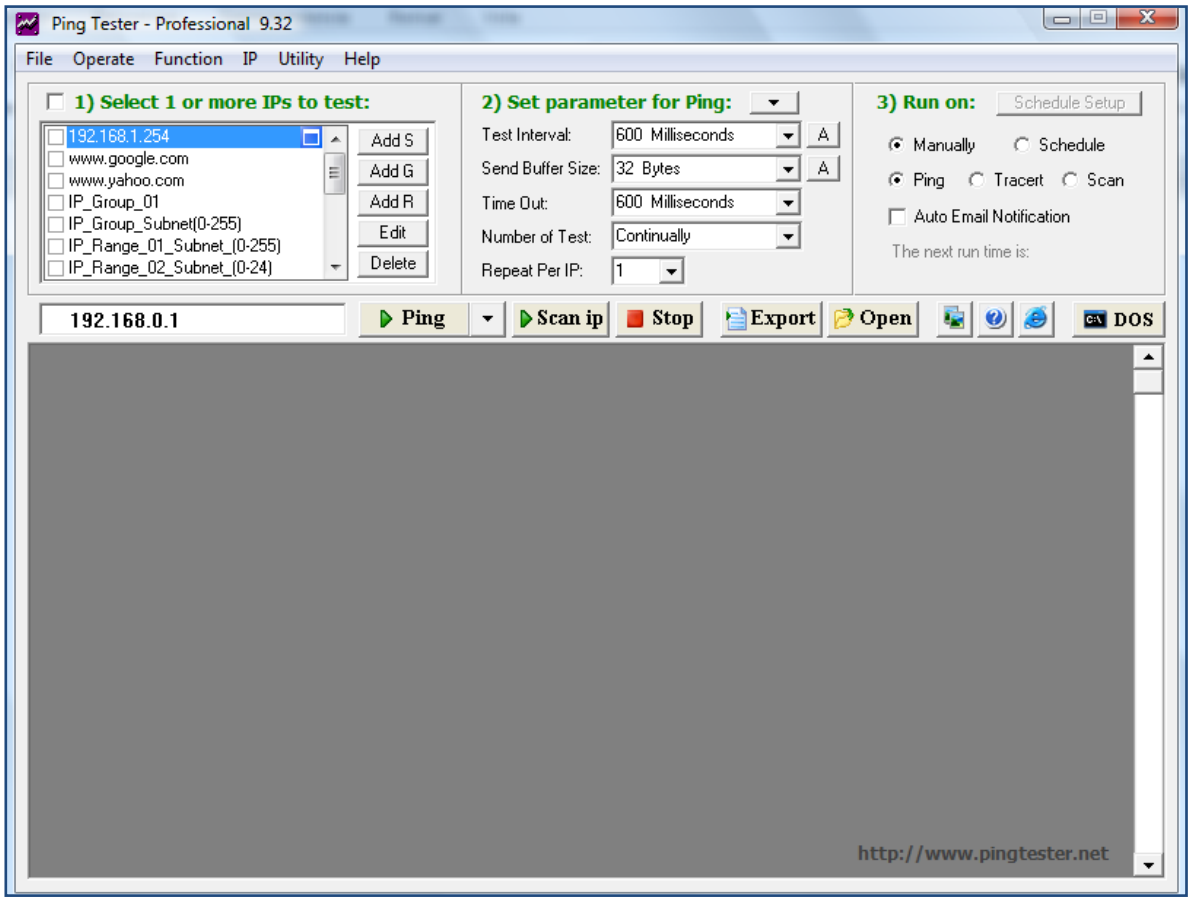

Figura 5.5. Interfaz principal de Ping Tester.
Fuente: (Ping Tester, 2014)

Se explica cómo es que se puede hacer ping (véase figura 5.6) a una IP en específico, a un grupo de IPs o a un rango de IPs; primero se hará una serie de pings hacia la página de Yahoo!, esta primer demostración se hace de manera manual, es decir, se selecciona la dirección IP que se le quiere hacer ping y después se le da en el  botón

Figura 5.6. Demostración de diez ping hacia el sitio de Yahoo!.
Fuente: (Ping Tester, 2014)

Otra de las opciones que ofrece esta herramienta es la de conocer también la ruta o camino que siguen los paquetes por medio de la opción Traceroute, para demostrar esto se vuelve hacer la prueba con el mismo servidor de Yahoo!.

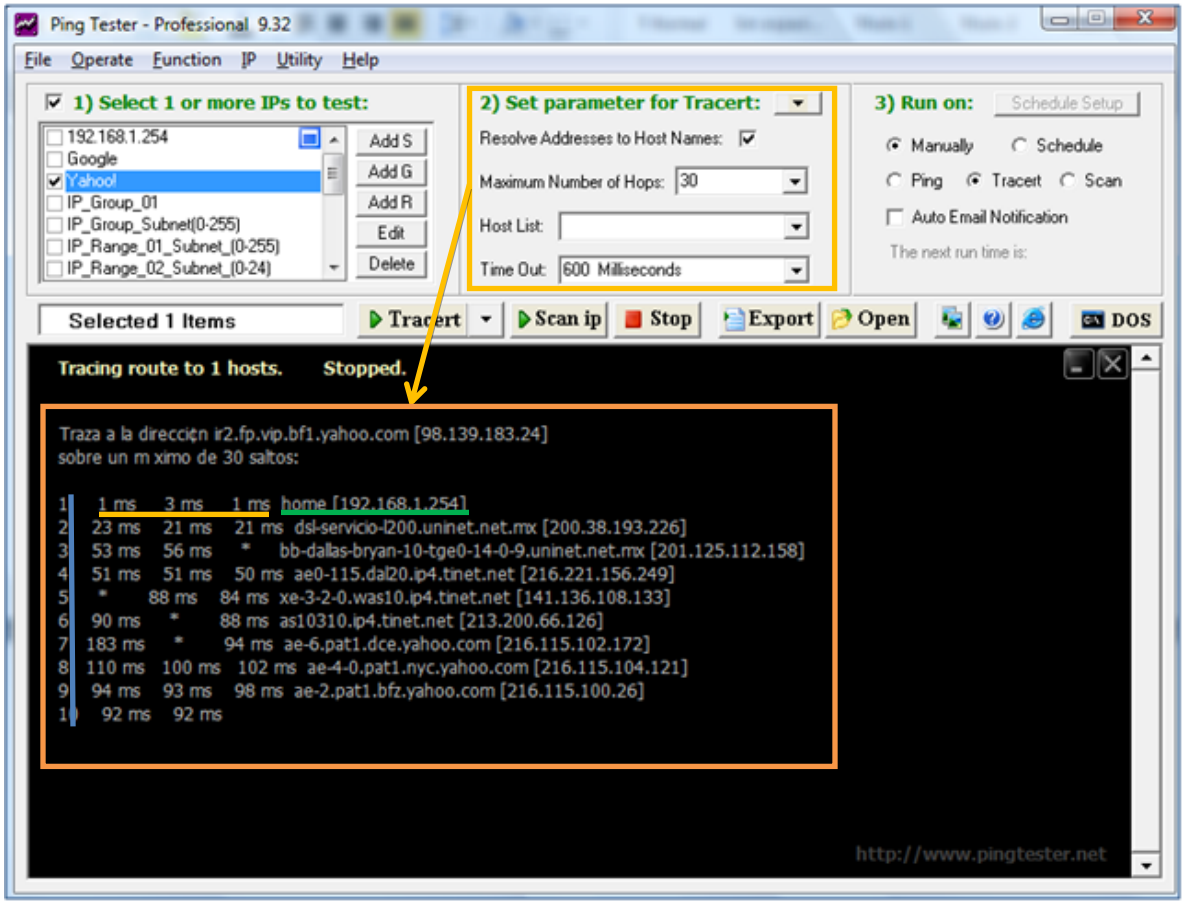

Figura 5.7. Traceroute de Yahoo!.
Fuente: (Ping Tester, 2014)

Ahora se va a explicar que es lo que significa los tiempos, las direcciones IP y la numeración que se muestra en el lado izquierdo (véase figura 5.7)[42]

La primer columna de izquierda a derecha (línea azul) son el número de saltos, después vienen tres tiempos (línea naranja) los cuales indican el tiempo de respuesta para los paquetes enviados mínimo, promedio y máximo, el asterisco indica que no se obtuvo respuesta alguna y en la última columna (línea verde) viene el nombre y la dirección IP del nodo por el que pasa el paquete.

Traceroute funciona gracias al campo TTL en los paquetes IP. Cada paquete IP posee un campo de tiempo de vida (TTL) útil el cual se reduce cada vez que pasa por un router. Cuando este campo llega a cero, el router determina que el paquete estuvo viajando en círculos, finaliza este paquete y envía una notificación ICMP

[42] Fuente: (Ping Tester, 2014)

(es un protocolo que permite administrar información relacionada con errores de los equipos en red, es usado por todos los routers para indicar un error) al remitente.

En esta tercera parte de la herramienta Ping Tester se demostrara como es que se puede enviar un ping o un traceroute de manera automática y enviar de manera automática las notificaciones por correo electrónico.

Como se muestra (véase figura 5.8) la programación para el envío de pings o de traceroute puede ser diario, semanal, mensual o por hora, solo se ajusta la hora en que se debe de enviar el ping, después se selecciona la carpeta destino en donde se guardaran los resultados de la prueba como se muestra (véase figura 5.9)

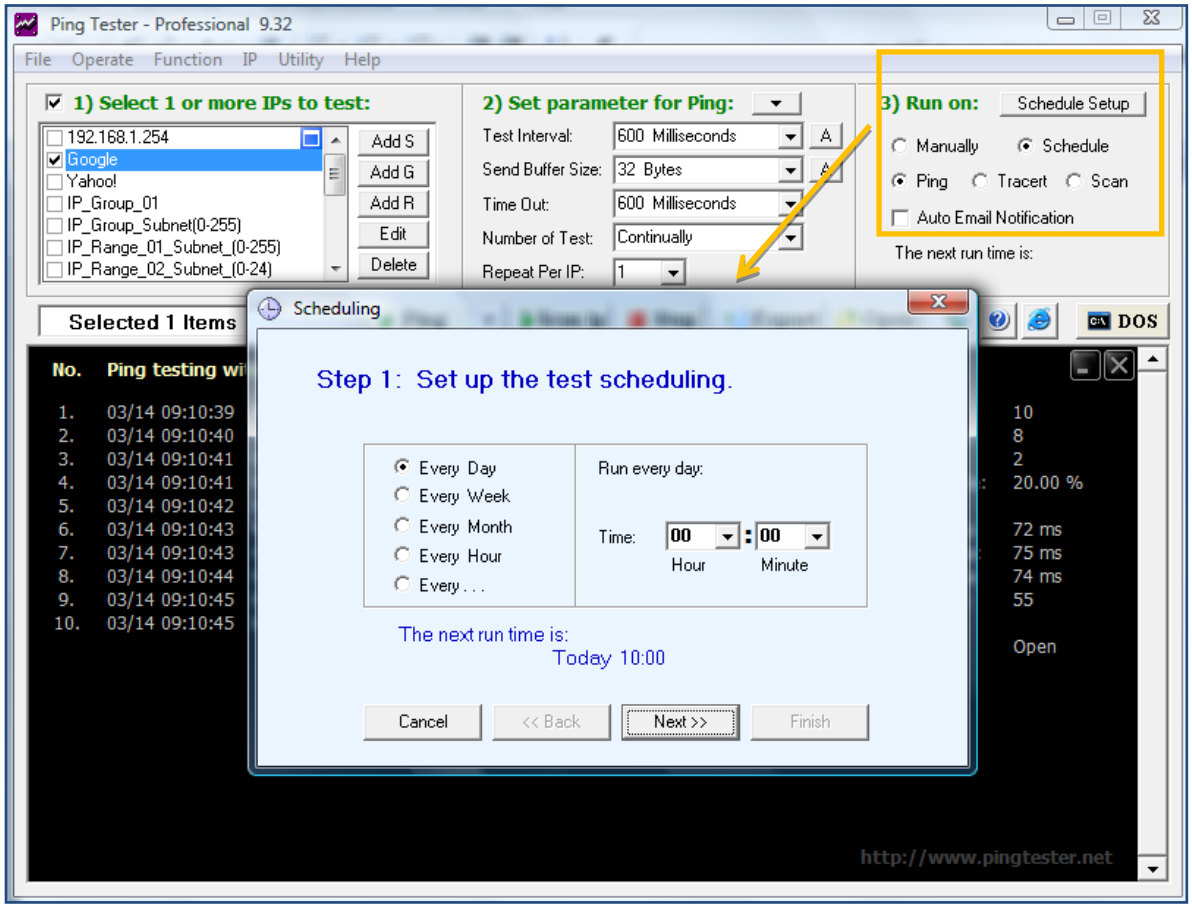

Figura 5.8. Programación del envío de pings o traceroute.
Fuente: (Ping Tester, 2014)

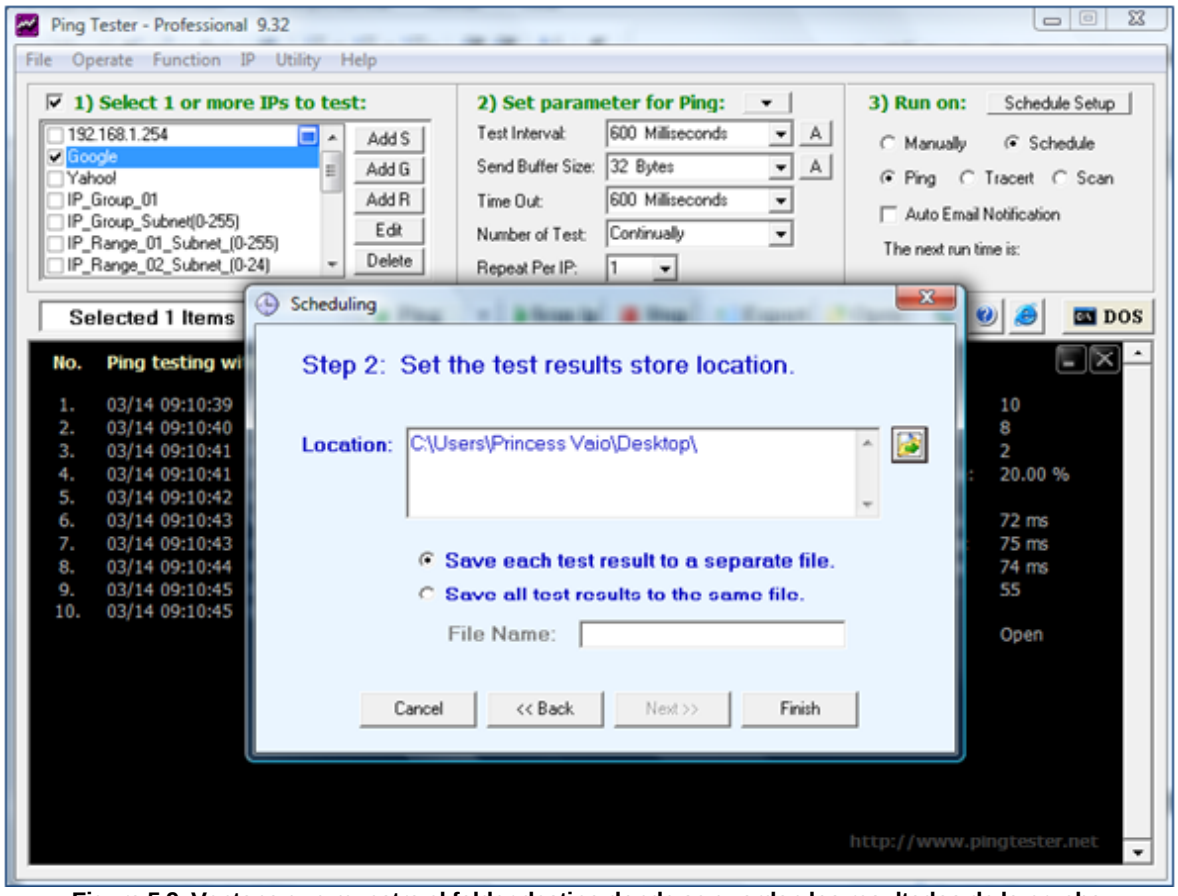

Figura 5.9. Ventana que muestra el folder destino donde se guardan los resultados de la prueba.
Fuente: (Ping Tester, 2014)

A continuación se muestran la (véase figura 5.10) con los resultados de una prueba realizada hacia Google, se puede apreciar la fecha y hora en la que inicio la prueba, el número de paquetes enviados, en esta prueba fueron cuatro así como los tiempos mínimo, máximo y promedio.

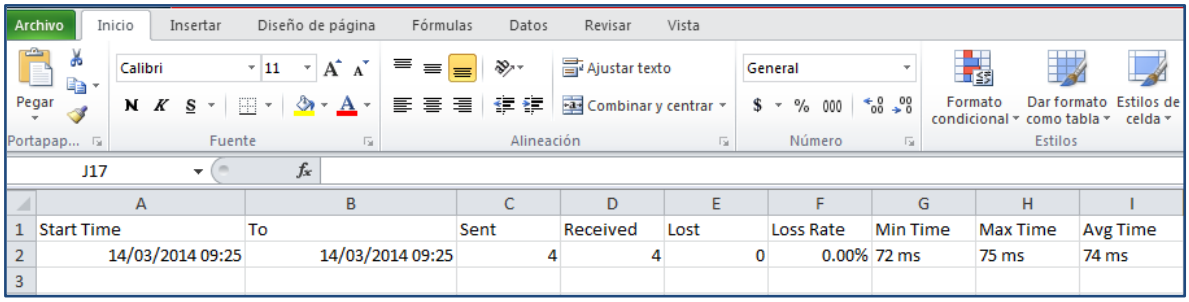

Figura 5.10. Resultados de la prueba de Ping Tester.
Fuente: (Microsoft Excel, 2014)

Por último se hará la demostración del envío de ping hacia algunos sistemas que están dentro de la red (véase figura 5.11) y estos son un teléfono con sistema Android con dirección IP 192.168.1.117, una máquina virtual con sistema operativo Fedora cuya dirección IP es 192.168.1.73 y una pantalla Bravia con dirección IP 192.168.1.69.

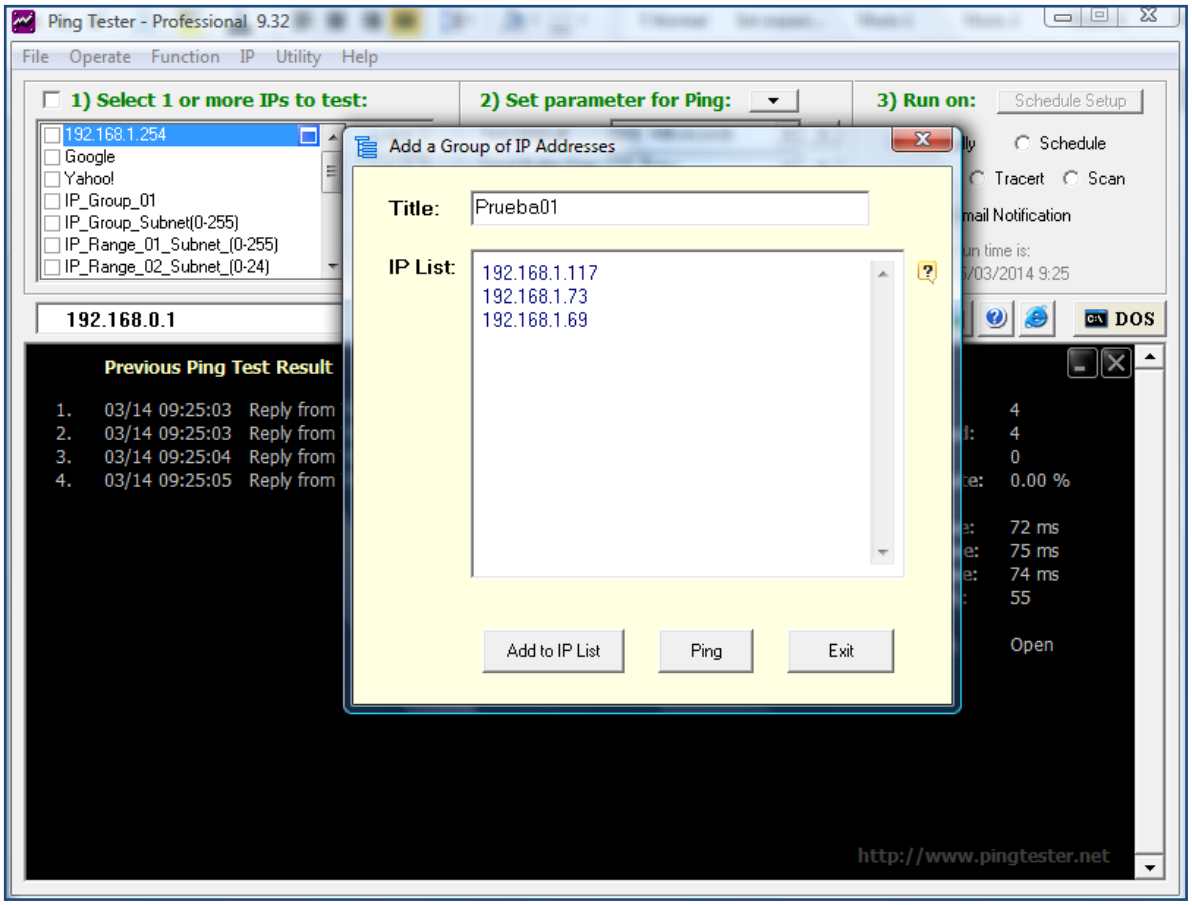

Figura 5.11. Creación de grupos de IPs para conocer su disponibilidad.
Fuente: (Ping Tester, 2014)

Se puede conocer qué dispositivos se encuentran activos dentro de la red por medio del botón *Scan IP* en base a esto se estableció un conjunto de IP que se colocaron en la figura anterior. Disponibilidad de los sistemas activos de los dispositivos mencionados anteriormente se muestran (véase figura 5.12)

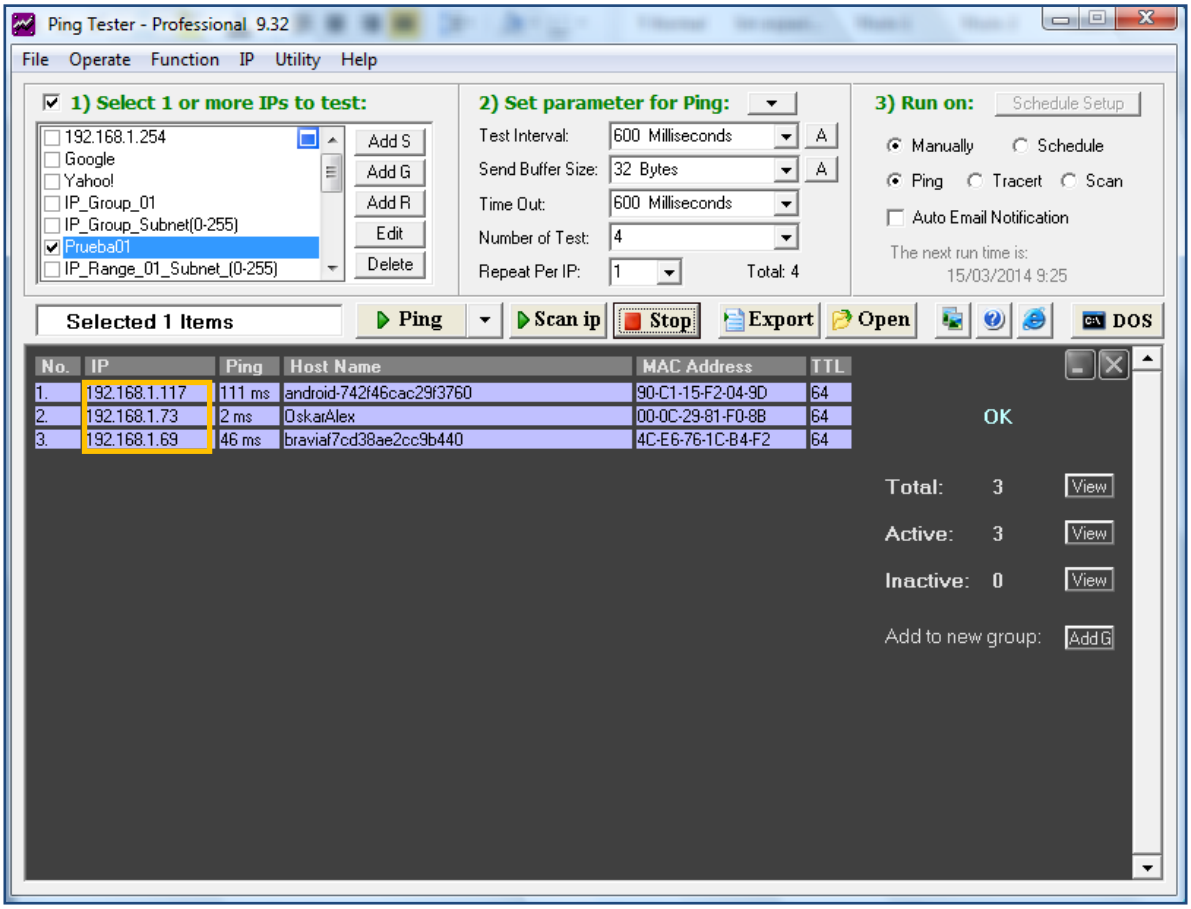

Figura 5.12. Escaneo de sistemas activos dentro de la red.
Fuente: (Ping Tester, 2014)

Ahora se continúa con el envío de los ping para ver si en verdad están activos estos dispositivos. Como se muestra (véase figura 5.13), los 3 sistemas se encuentran activos.

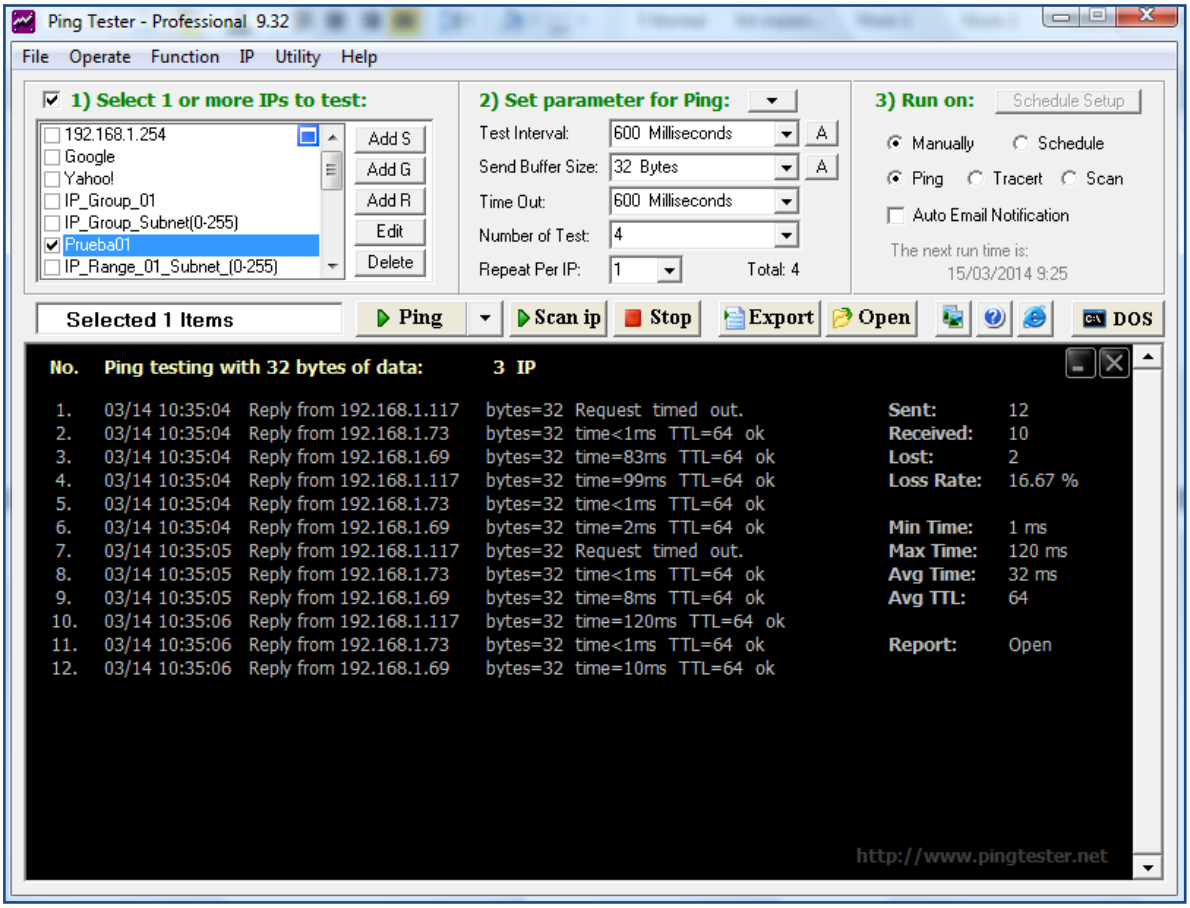

Figura 5.13. Resultado de la prueba de 3 dispositivos.
Fuente: (Ping Tester, 2014)

Por último se muestra el *traceroute* (véase figura 5.14) de esos 3 sistemas y se observa que en los 3 casos se completa satisfactoriamente. Con base en estos resultados que se hicieron se puede concluir que Ping Tester es una buena herramienta que será de gran utilidad cuando se necesita conocer si los sistemas que se encuentran dentro de la red están activos.

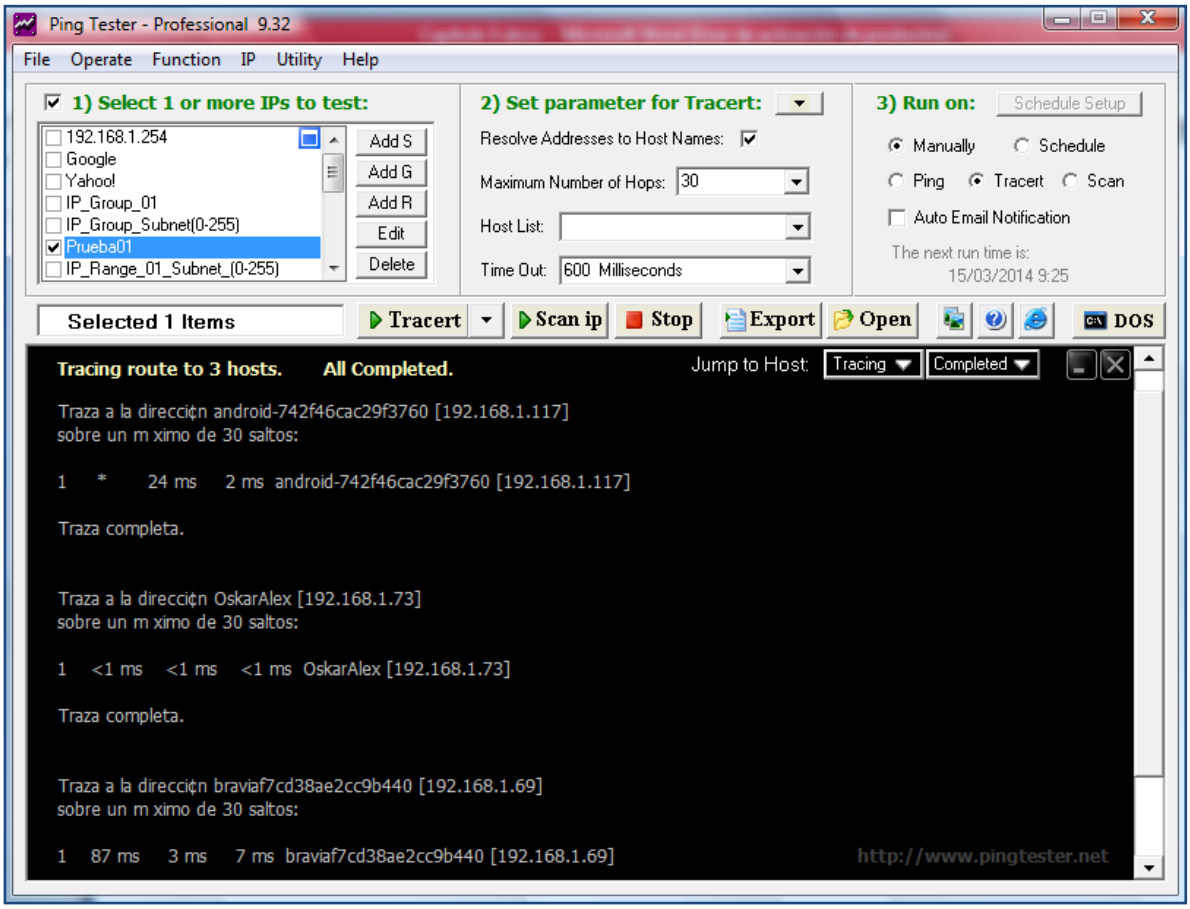

Figura 5.14. Traceroute de los 3 dispositivos activos en red.
Fuente: (Ping Tester, 2014)

5.3 PASOS PARA CREAR UN TICKET Y NOTIFICAR UN INCIDENTE CON RTIR (REQUEST TRACKER FOR INCIDENT RESPONSE)

En esta parte de la investigación se muestra paso a paso como crear un *ticket* para enviar una notificación al área correspondiente, en este caso al área de seguridad informática, utilizando el gestor de incidente RTIR (Request Tracker for Incident Response), a continuación (véase figura 5.15) se muestra la página de inicio de sesión de RTIR donde se encuentran los campos de "Usuario" y "Password".

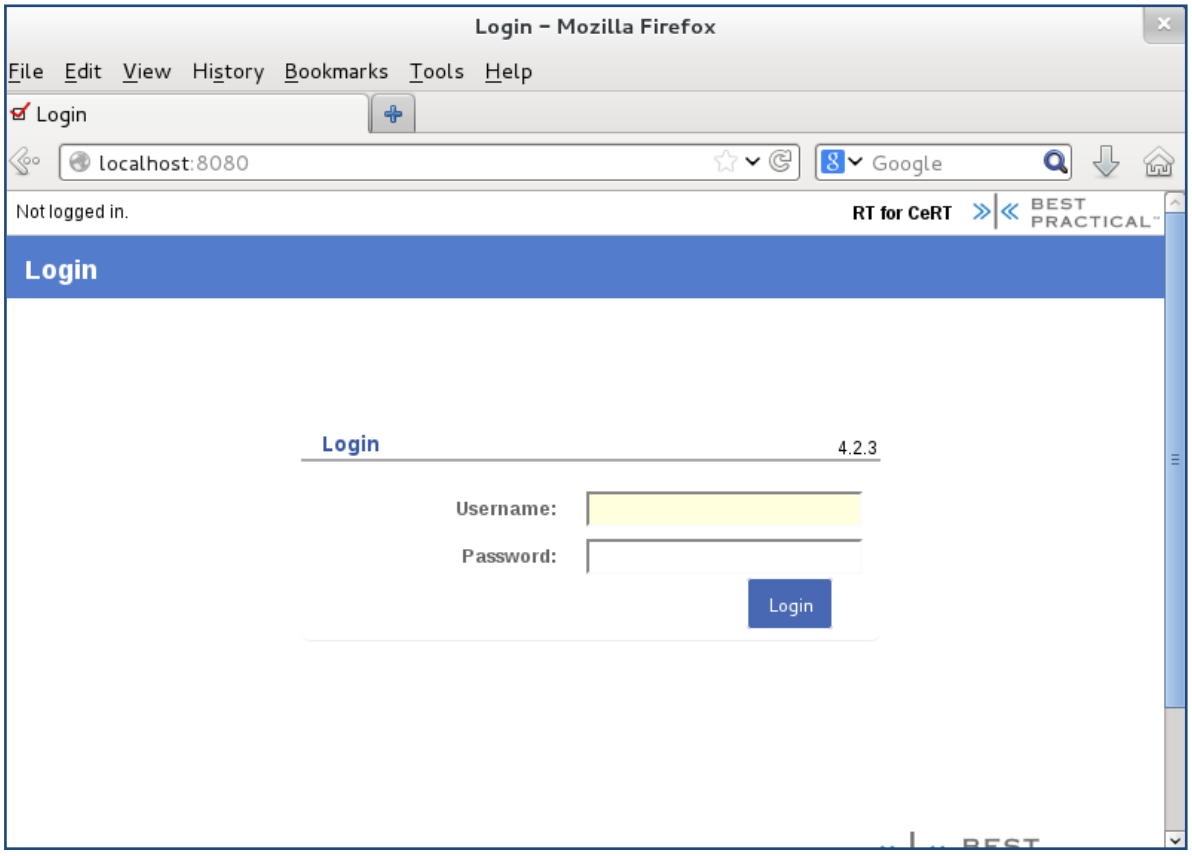

Figura 5.15. Página de inicio de RTIR
Fuente: (RTIR, 2014)

Las credenciales para iniciar *root* son:

- Username: OscarAle
- Password: password

Como se puede observar la contraseña es *password,* este valor no fue modificado ya que solo es para fines demostrativos, además de que es la contraseña por *default* de RTIR cuando se instala, lo más recomendable es cambiarla, para así evitar futuros problemas.

Una vez iniciado RTIR en modo *root* (véase figura 5.16), así es como se ve la página principal del gestor de incidentes.

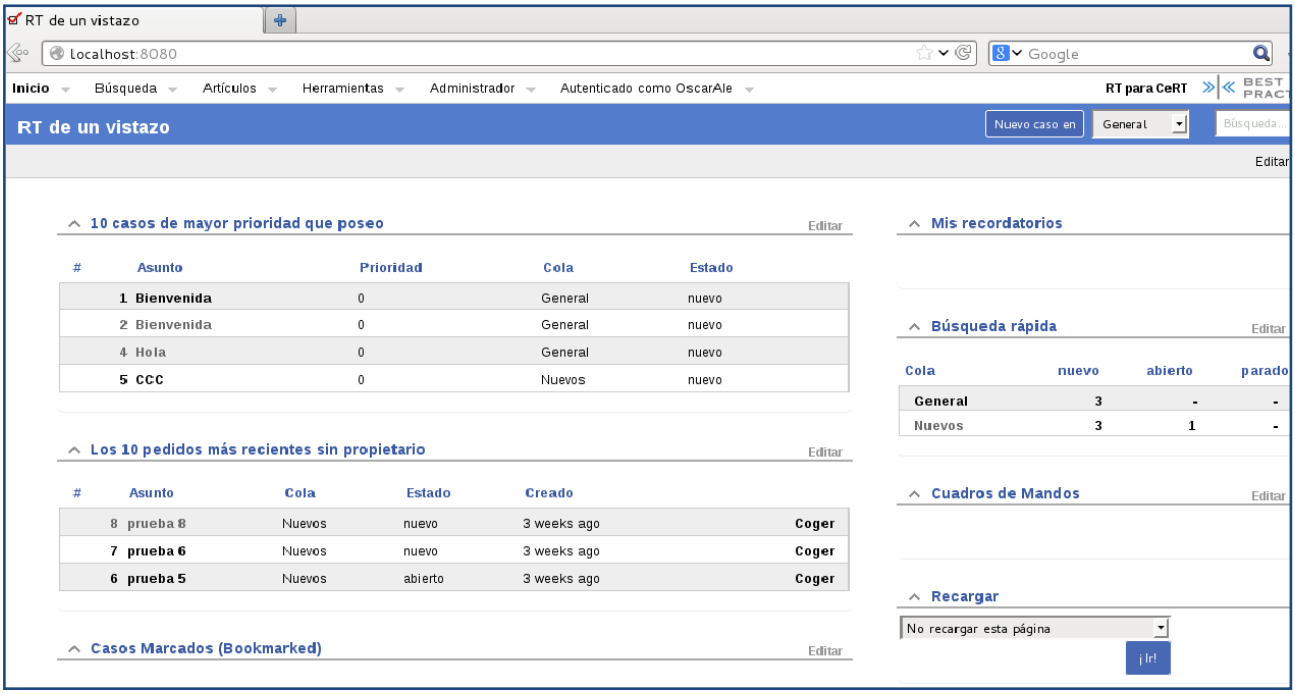

Figura 5.16. Página principal de RTIR.
Fuente: (RTIR, 2014)

Una vez aquí, se crea un usuario que sirve para demostrar cómo es que se debe de crear un *ticket*, en el campo “Administrador” se selecciona “Usuarios” y después “Crear”, (véase figura 5.17)

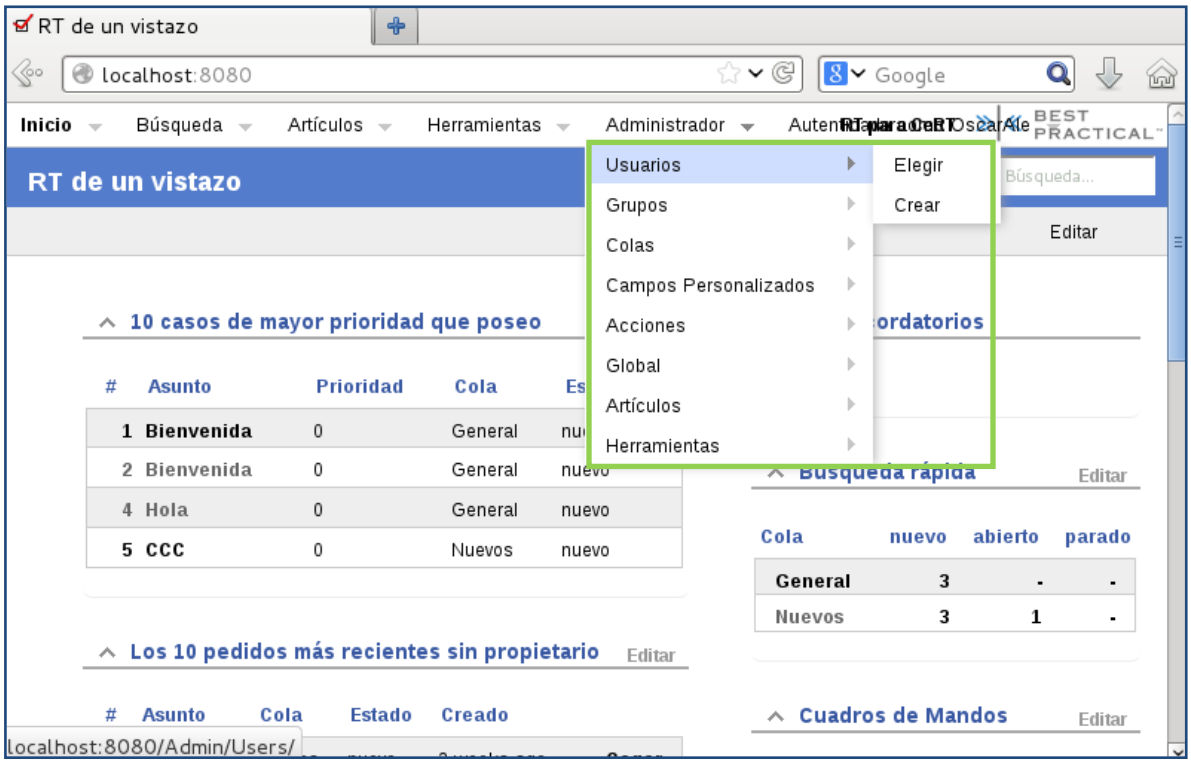

Figura 5.17. Creación de un usuario para demostración de creación de *ticket*.
Fuente: (RTIR, 2014)

Ahora se llenan todos los campos con la información correspondiente y marcar en "Control de Acceso" la opción de "Privilegiado" (véase figura 5.18)

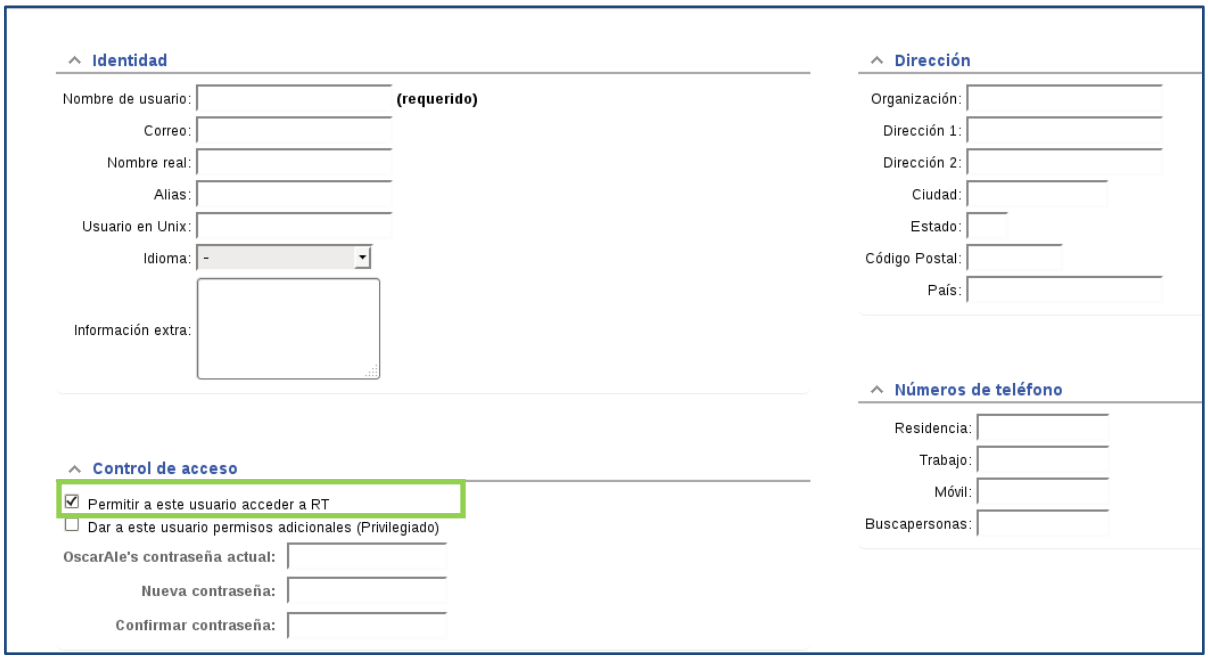

Figura 5.18. Campos para crear un nuevo usuario.
Fuente: (RTIR, 2014)

Una vez hecho lo anterior se da “Crear” es resultado (véase figura 5.19)

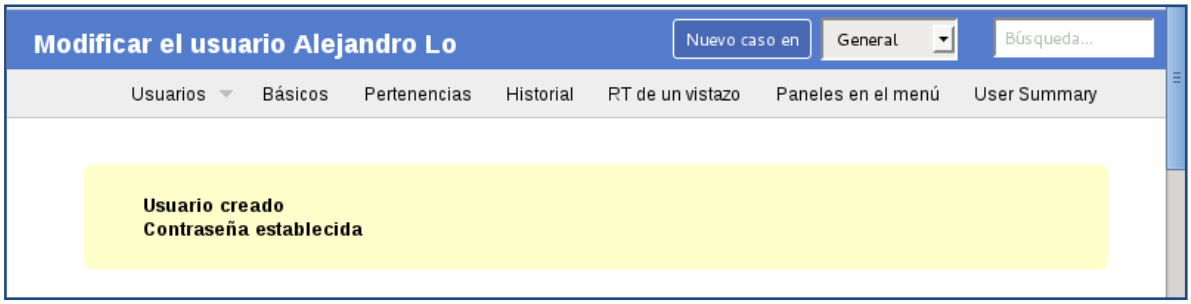

Figura 5.19. Usuario creado y contraseña establecida.
Fuente: (RTIR, 2014)

Ahora en esta siguiente parte se crea un grupo que contenga varios usuarios ya que es más eficiente administrar privilegios por grupo que por usuario, dentro de la misma opción de “Administrador” seleccionar “Grupo” y después “Crear” (véase figura 5.20)

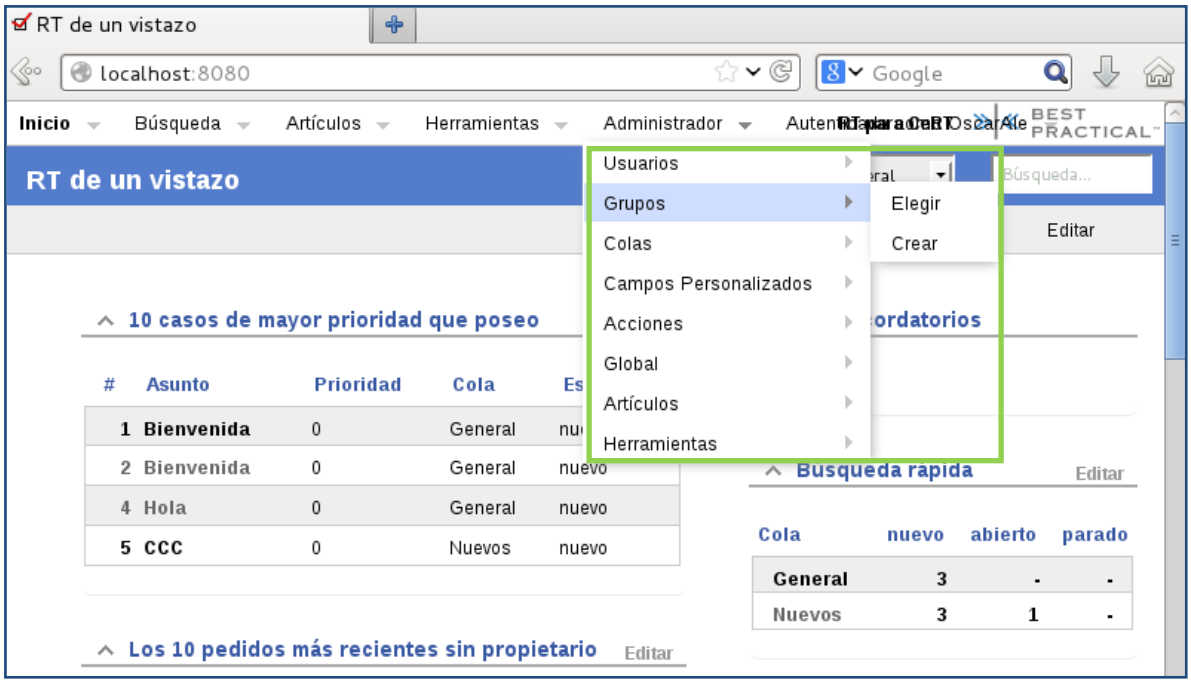

Figura 5.20. Creación de un grupo.
Fuente: (RTIR, 2014)

Se llenan los correspondientes campos y se da una breve descripción del grupo, después se le da “Crear” y listo, se tiene el primer grupo (véase figura 5.21)

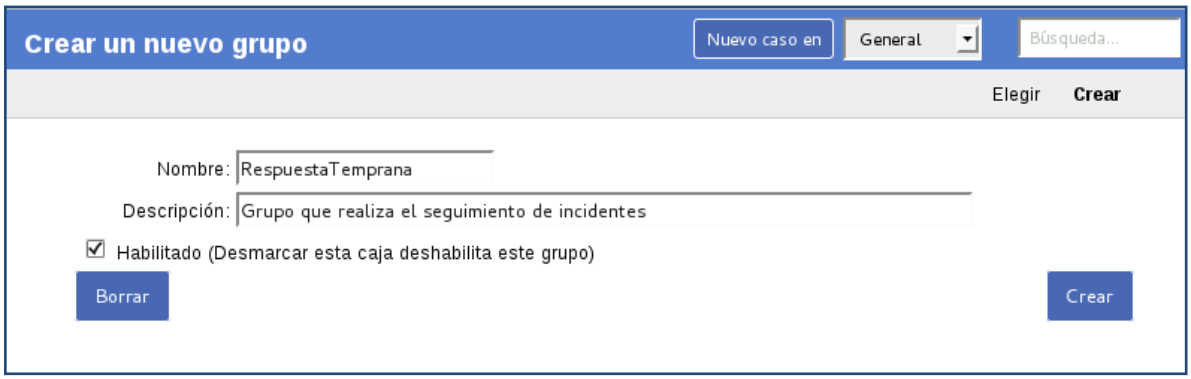

Figura 5.21. Creación de un grupo.
Fuente: (RTIR, 2014)

Ahora se agregarán miembros al grupo llamado *Respuesta Temprana*, en ese grupo se agregará al que será el SysAdmin, una vez seleccionado los campos necesarios se le da “Guardar Cambios”, (véase figura 5.22)

Figura 5.22. Selección de privilegios para el SysAdmin.
Fuente: (RTIR, 2014)

Ahora el siguiente paso es crear una “Cola”, esto sirve para categorizar los problemas como por ejemplo: seguridad, cuentas y conectividad; asignación de usuarios.

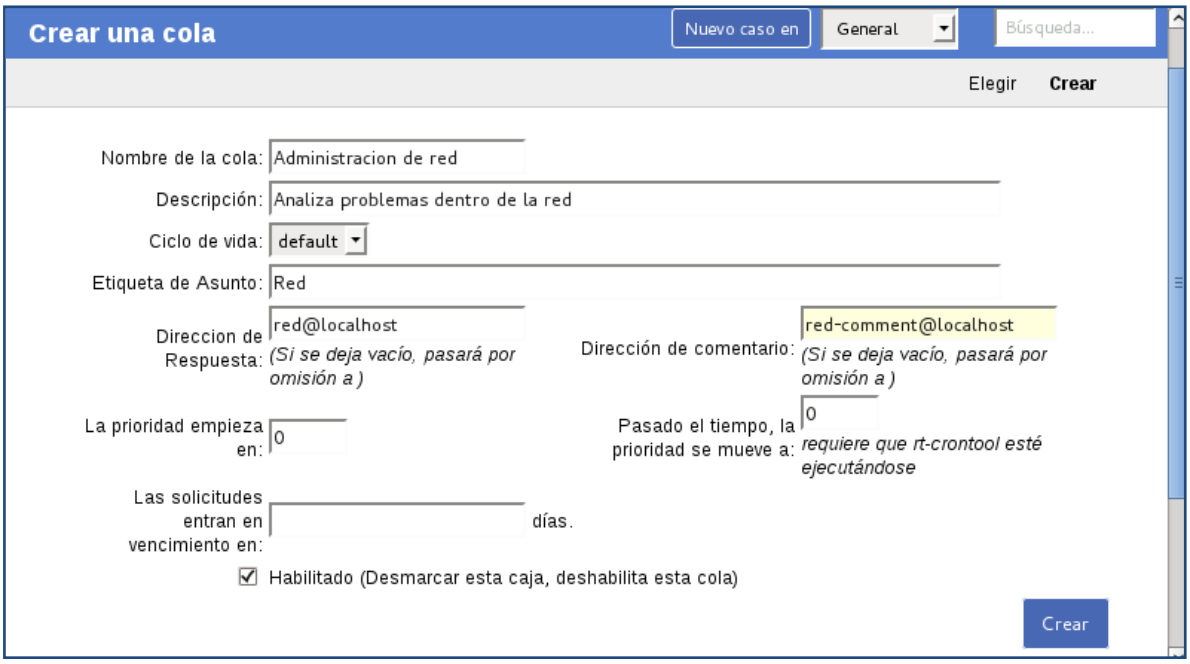

Figura 5.23. Llenado de campos en la creación de una cola.
Fuente: (RTIR, 2014)

Una vez creado la “Cola” se le asignaran permisos, los permisos a seleccionar son:

- Crear casos.
- Responder a los casos.
- Ver Cola.
- Ver resumen del caso.

Estas opciones se seleccionan en el campo de “Todos” que se encuentra en la parte izquierda (véase figura 5.23), una vez hecho esto se da clic en “Guardar Cambios”.

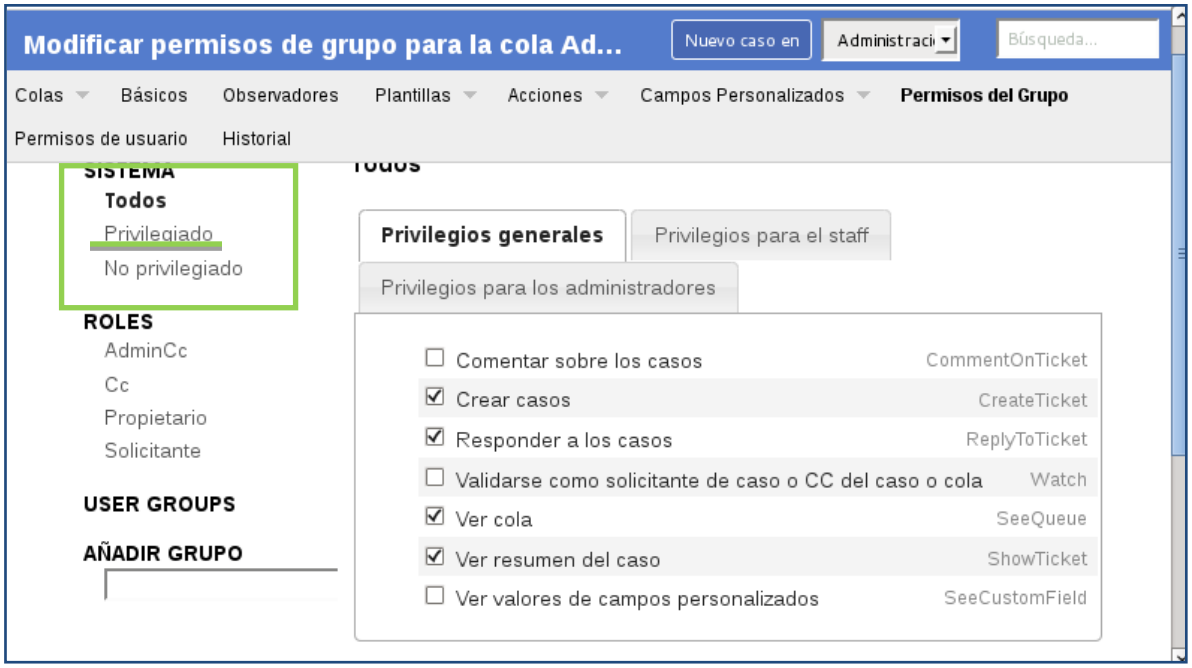

Figura 5.24. Asignando privilegios de la cola administración de red.
Fuente: (RTIR, 2014)

Una vez seleccionado los privilegios (véase figura 5.24) se cierra sesión y se inicia de nuevo con el usuario *SysAdmin*, en este caso es *Alejandro Lo* con el mismo password que el usuario anterior.

A continuación se muestra (véase figura 5.25) la página de inicio con el nuevo usuario, se puede ver en la parte superior el nombre de dicho usuario el cual será el nuevo *SysAdmin* del gestor de incidentes.

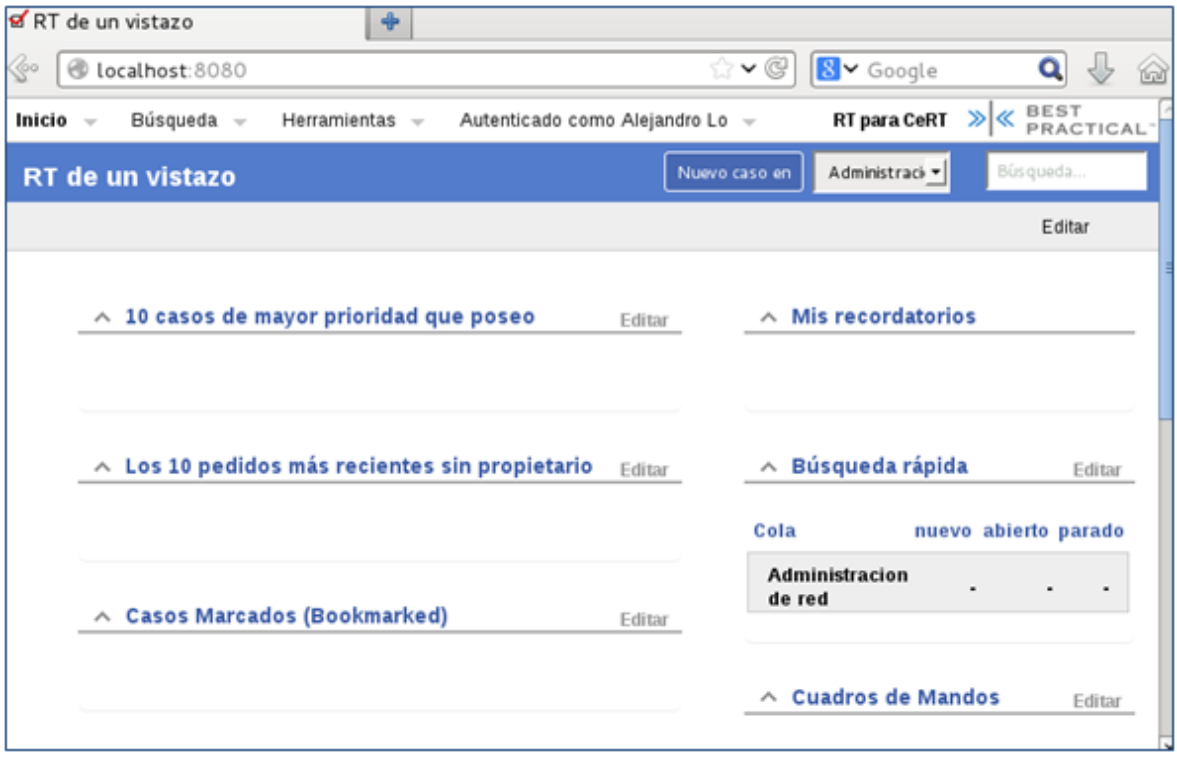

Figura 5.25. Página de inicio.
Fuente: (RTIR, 2014)

Lo siguiente es crear un *ticket* para darle seguimiento al incidente, el cual consiste en ver, responder, resolver y reabrir un *ticket*. Lo primero es dar clic en el campo de “Crear Nuevo Caso” (véase figura 5.26)

Figura 5.26. Creación de un nuevo caso.
Fuente: (RTIR, 2014)

Se deben de colocar en los campos correspondientes (véase figura 5.26) el correo electrónico de las personas que se van a encargar del caso, así como el asunto, una breve descripción del incidente e inclusive se puede adjuntar algún documento que sustente el problema o que dé a conocer las causas que provocaron el incidente, para que sea más rápido la solución.

Una vez establecido lo anterior se da clic en el botón “Crear”. Ya que esta creado el *ticket* se da clic sobre éste y mostrará el contenido del mismo (véase figura 5.27)

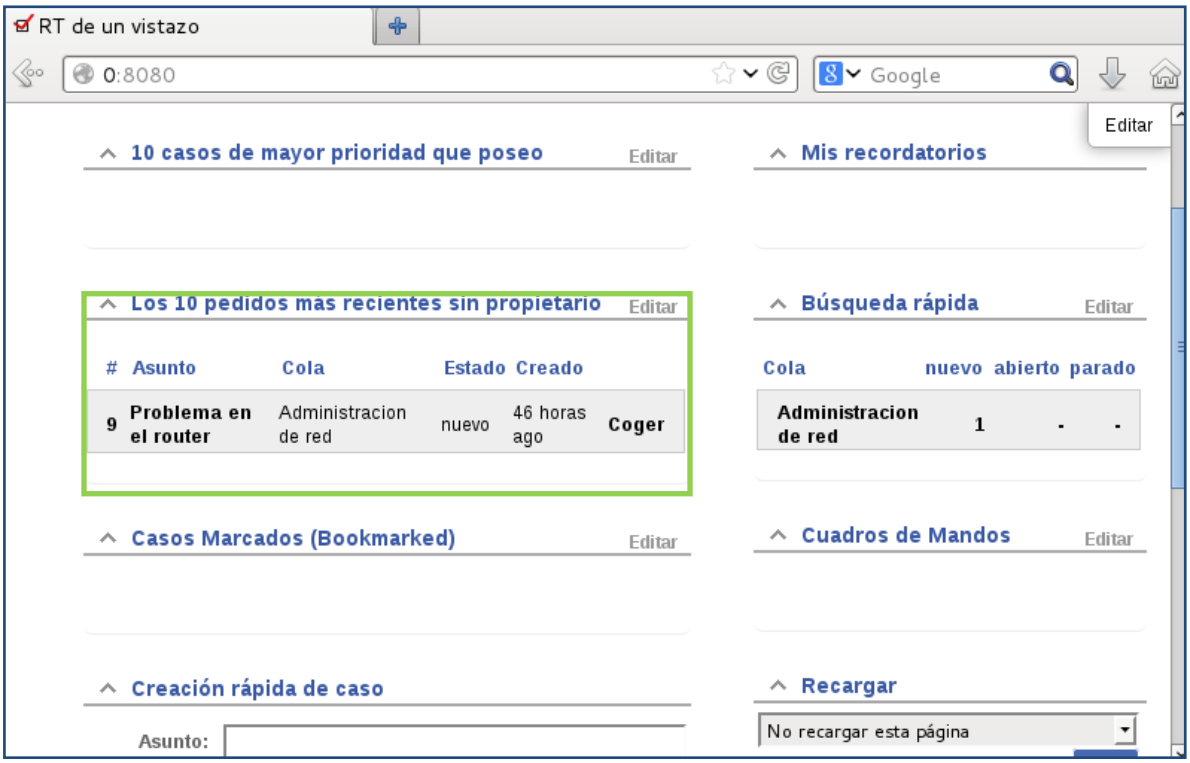

Figura 5.27. Ticket llamado “Problema en el router”.
Fuente: (RTIR, 2014)

Después se selecciona “responder” y se hacen las debidas anotaciones del avance del caso, si el caso se resolvió, el estado del caso se pone en “resuelto” como se muestra (véase figura 5.28)

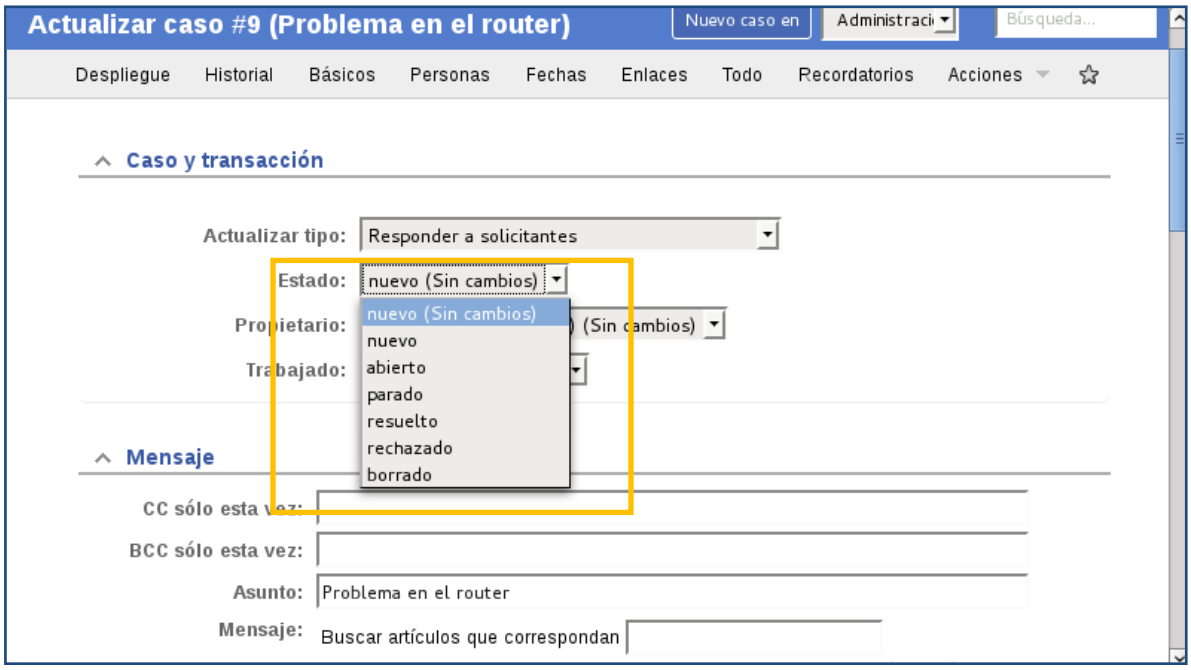

Figura 5.28. Opciones del estado del caso.
Fuente: (RTIR, 2014)

Después de haber seleccionado el estado del caso se da clic en “Actualizar Caso”, y muestra lo siguiente (véase figura 5.29)

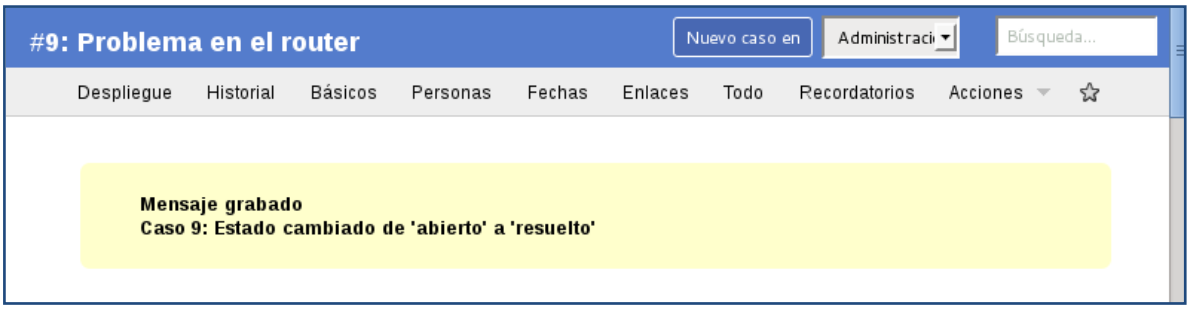

Figura 5.29. Solución del caso.
Fuente: (RTIR, 2014)

Ahora por último si se quiere hacer una búsqueda (véase figura 5.30) de un elemento dentro de una cola, se selecciona “búsqueda”, después se va hacia “añadir criterio”, dentro de la opción “cola” seleccionar “administración de red”.

Figura 5.30. Búsqueda de elementos dentro de una cola.
Fuente: (RTIR, 2014)

Después se da clic en “agregar términos y buscar”, mostrará (véase figura 5.31), los resultados de la búsqueda aparecerán de manera similar a como se muestra en la imagen. Aquí se podrán ver los *tickets* que están cerrados, resueltos, etc.

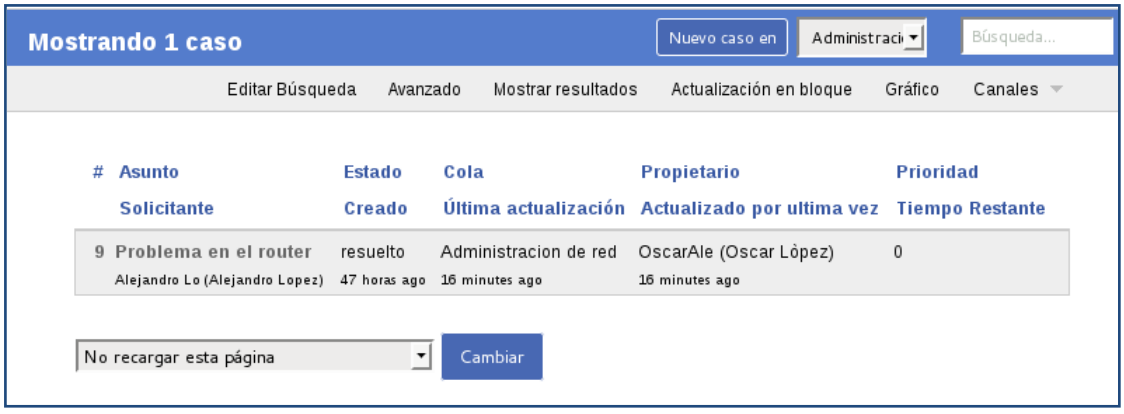

Figura 5.31. Caso resuelto.
Fuente: (RTIR, 2014)

5.4 MOSTAR ACTIVIDAD DE ATAQUES EN SNORBY DE MODO GRÁFICO (DASHBOARD)

En esta última parte de la investigación se muestra como es que se pueden identificar las intrusiones a la red de cualquier organización con el fin de robar información, se realizaran varios ataques con la finalidad de que el IDS/IPS Snort pueda detectarlos y por medio de la interfaz Snorby se puedan interpretar e inclusive categorizar según la severidad del ataque.

El primer ataque a recrear es un escaneo de puertos hacia la maquina víctima, la herramienta a utilizar es Nmap, los tipos de escaneo que puede realizar esta herramienta son:[43]

- Escaneo de redes: Permite conocer los dispositivos conectados a la red.
- Escaneo de puertos: Permite conocer que puertos de las maquinas conectadas a una red y ver si se encuentran abiertos, lo cual permitirá poder colarse por uno de ellos en caso de que se encuentren abiertos.
- Escaneo de vulnerabilidades: Permite identificar servicios vulnerables de las maquinas conectadas a la red que permitan la entrada al sistema.

Nmap es muy flexible porque soporta docenas de técnicas avanzadas para el mapeo de las redes llenas de filtros IP, cortafuegos, routers y otros obstáculos.

Nmap funciona enviando paquetes o realizando una llamada de conexión, cuando se realiza esto Nmap puede distinguir seis estados para cada puerto:[44]

- Abierto: Existe una aplicación que acepta conexiones TCP, datagramas UDP asociaciones SCTP en el puerto.
- Cerrado: Se puede tener acceso al puerto pero no hay ninguna aplicación escuchando en ese puerto.
- Filtrado: Los paquetes enviados han sido filtrados por un firewall, algunas reglas de un router, lo cual impide a Nmap determinar si está abierto o no ese puerto.
- Sin filtrar: El puerto es accesible pero Nmap no puede determinar si está abierto o cerrado el puerto, y devuelve un ACK.

[43] (Taringa, 2013)
[44] (Hackers, 2012)

- Abierto/filtrado-cerrado/filtrado: Nmap no puede saber a ciencia cierta si el puerto está cerrado, abierto o filtrado. Esto sucede cuando los puertos abiertos no generan una respuesta.

Para establecer la conexión se debe seguir un procedimiento llamado 3 way handshake como se muestra (véase figura 5.32)

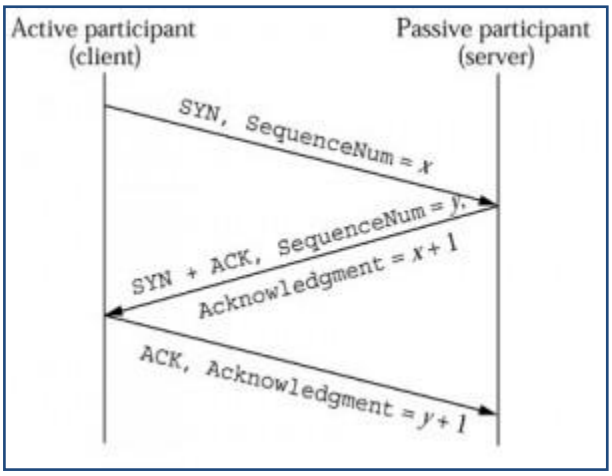

Figura 5.32. Procedimiento 3 way handshake.
Fuente: (Taringa, 2013)

Lo que viene a decir es que el cliente envía un TCP SYN (con un número de secuencia asignado para evitar Spoofing), si el puerto está abierto el servidor responde con un SYN/ACK, en caso contrario el servidor envía un paquete con el flag RST activado, y el cliente responde al servidor con un ACK, completando así la conexión.

La sintaxis de Nmap seria:

```
# nmap (opción_escaneo) (maquina_escanear)
```

A continuación se enuncian algunos tipos de escaneos.[45]

Escaneo TCP SYN: Consiste en enviar un paquete SYN y espera la respuesta del servidor, si llega a recibir un SYN/ACK el puerto estará abierto, en caso de que solo llegue a recibir un SYN sin el ACK también se considera que el puerto está abierto, si

[45](Hackers, 2012)

recibe un RST el puerto está cerrado y si no recibe ninguna respuesta se considera filtrado.

```
# nmap –sS (máquina)
```

Escaneo TCP connect: Nmap pide al sistema que establezca una conexión con la máquina destino a través del puerto elegido mediante una llamada tipo *connect*. Se trata de una opción menos eficiente que TCP SYN, porque requiere más tiempo y más paquetes para obtener la misma información que se obtiene con el escaneo TCP SYN.

```
# nmap –sT (máquina)
```

Escaneo UDP: Muchas veces no se utiliza este tipo de escaneo por ser lento y difícil a comparación de TCP, pero se debe de considerar importante este tipo de escaneo ya que el DNS (puerto 53), SNMP (puertos 161/162) y DHCP (puertos 67/68), cliente-servidor están abiertos estos puertos. Funciona mediante el envío de paquetes UDP a los puertos seleccionados, cuando se devuelve un error “ICMP unreachable”, el puerto está cerrado o filtrado y si hay alguna respuesta mediante un paquete UDP el puerto estará abierto.

```
# nmap –sU (máquina)
```

Escaneo SCTP INIT: Es una alternativa de los escaneos de TCP y UDP, sería similar a un TCP SYN pero en SCTP (Stream Control Transmission Protocol), este protocolo provee confiabilidad, control de flujo y secuenciación como TCP.
Este tipo de escaneo es rápido, es poco intrusivo, hace diferencia entre los estados de los puertos (abierto, cerrado y filtrado), no completa la asociación SCTP porque envía un paquete INIT con la finalidad de pretender abrir una conexión y espera la respuesta con un INIT-ACK (puerto abierto), si recibe un ABORT el puerto estará cerrado y si no hay respuesta alguna el puerto esta filtrado.

```
# nmap –sY (máquina)
```

Escaneo TCP personalizado: Permite al usuario elegir qué tipo de bandera utilizará para el escaneo (URG, ACK, PSH, RST, SYN, FIN).

```
# nmap –sF/sA –scanflags URG
```

Se muestra un ejemplo de cómo se ve Snorby (véase figura 5.33) cuando se hace un escaneo de puertos, muestra la IP de origen y la IP destino, así como la fecha de cuando se realizó ese escaneo.

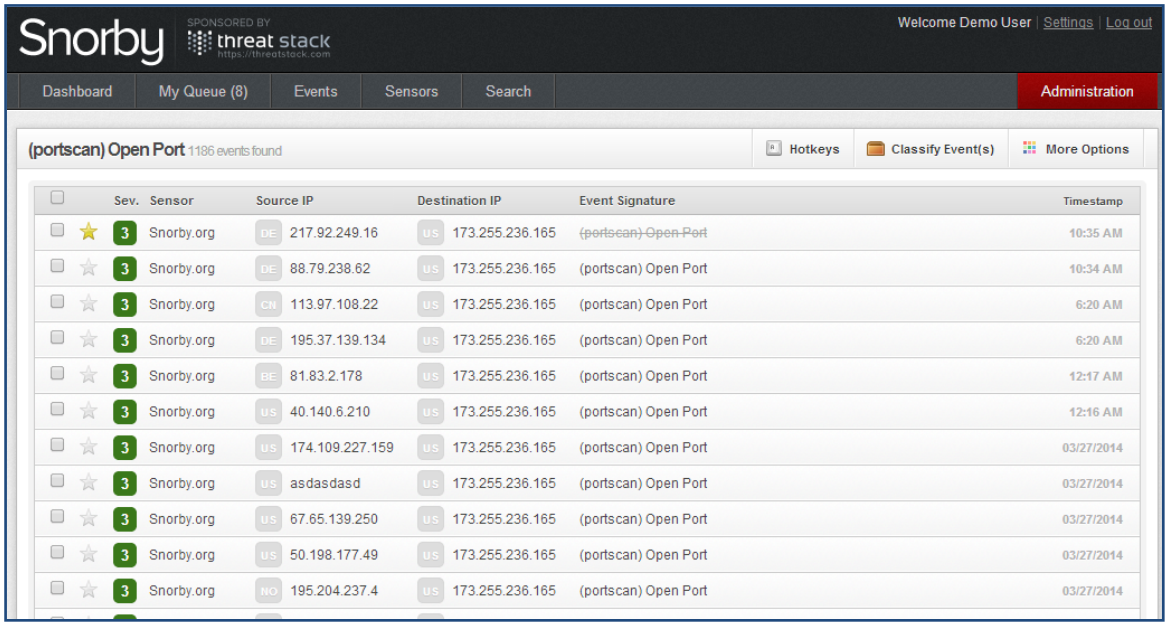

Figura 5.33. Tabla que muestra el portscan con IPs destino y origen.

Pero antes de continuar se muestra la página principal de Snorby, (véase figura 5.34) Como se puede observar está integrado por 3 partes, la primera muestra el grado de gravedad del ataque realizado, esto son *high severity, medium severity* y *low severity* (cuadro azul), también muestra el periodo en que ocurrieron esos ataque y van desde las últimas 24 horas hasta 1 año; en la segunda parte muestra y es aún más interesante porque muestra de manera gráfica el conteo de eventos contra el tiempo en el que ocurrieron, como se muestra en la imagen (cuadro verde), las tres primeras

pestañas que son *sensors, severities* y *protocols,* son gráficas de líneas, y las otras tres son gráficas de pastel que son la de *signatures, sources* y *destinations* (cuadro verde); y la tercera parte que es la columna de la derecha muestra el número de eventos registrados como un top de los últimos 5 usuarios activos, después los 5 eventos únicos y al final la clasificación de eventos los cuales son *acceso a root no autorizado, falsos positivos, atentados de acceso no autorizado, ataques de denegación de servicios, reconocimiento, infección de virus, violación de políticas y acceso de usuarios no autorizados* (cuadro rojo)

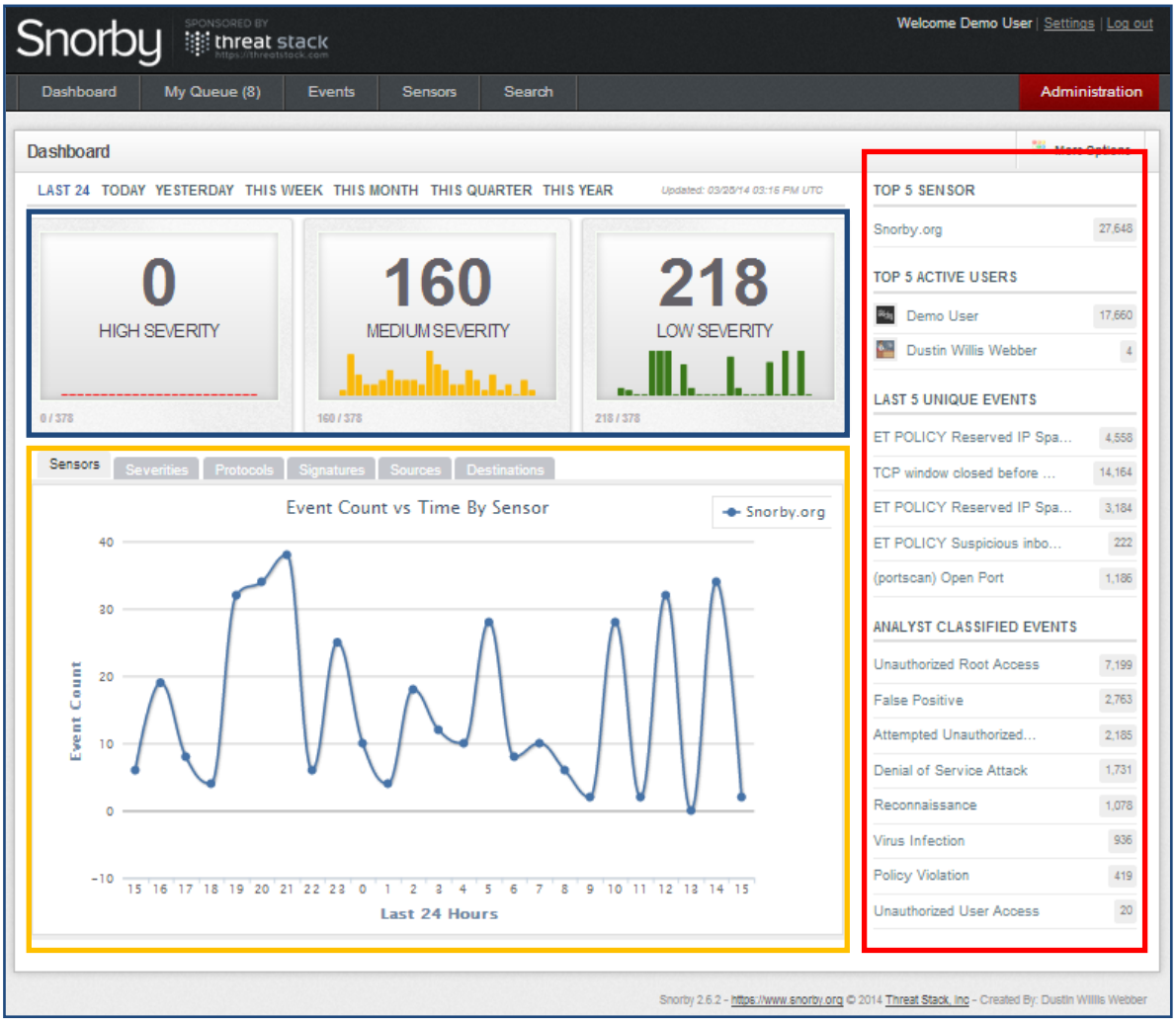

Figura 5.34. Página principal de Snorby.
Fuente: http://demo.snorby.org/

Ahora se selecciona un evento de gravedad media (véase figura 5.35) para conocer más acerca de ese evento, dentro de ese apartado se muestra información detallada como las cabeceras IP, información de la firma, información de cabeceras TCP, referencias, cargas útiles y en el último apartado se puede poner algún comentario acerca del evento.

Se muestra (véase figura 5.36) un registro clasificado como “infección de virus”, aquí se muestra la información de cabeceras IP, información de la firma, la carga de ese virus o *payload.*

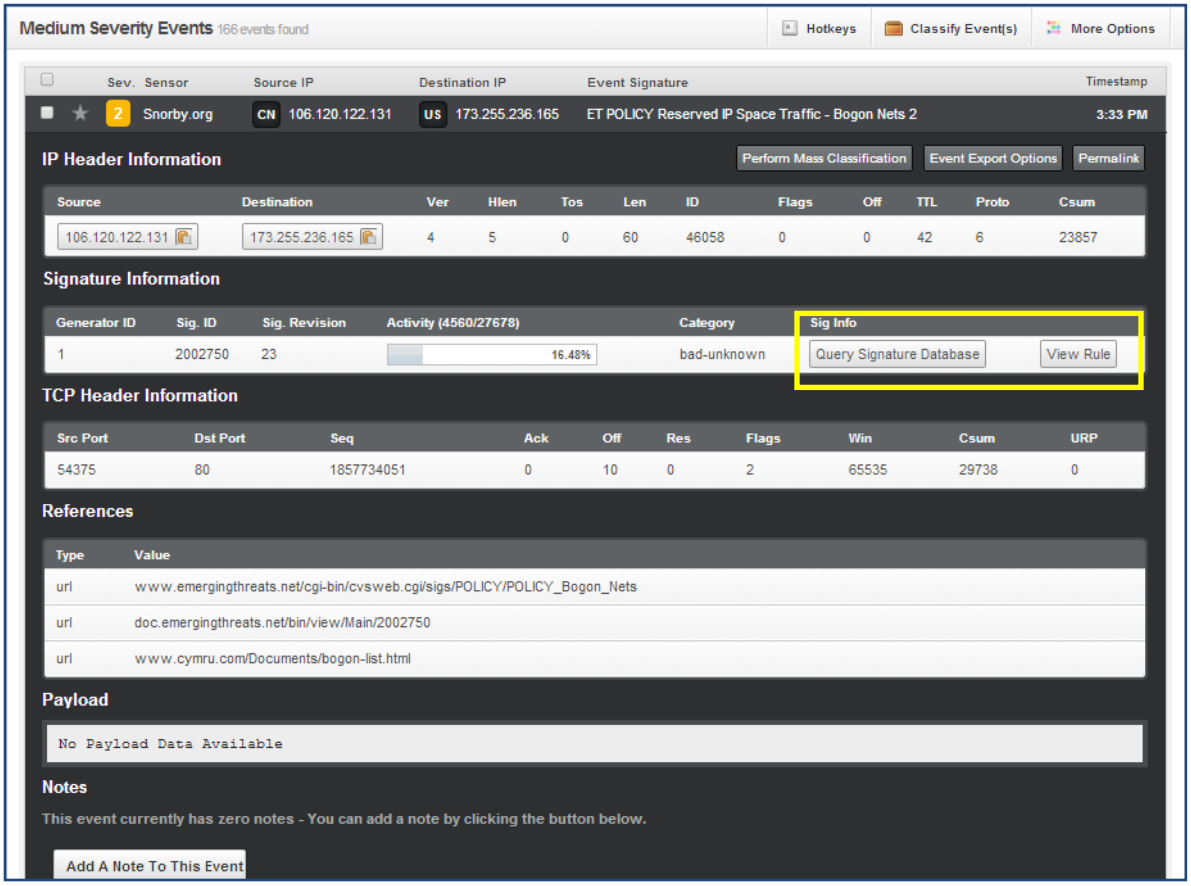

Figura 5.35. Información detallada de un evento de mediana gravedad.
Fuente: http://demo.snorby.org/

Dentro de la sección de “información de la firma” se puede encontrar información de “bases de datos de firma de consulta” y “reglas” (cuadro amarillo)

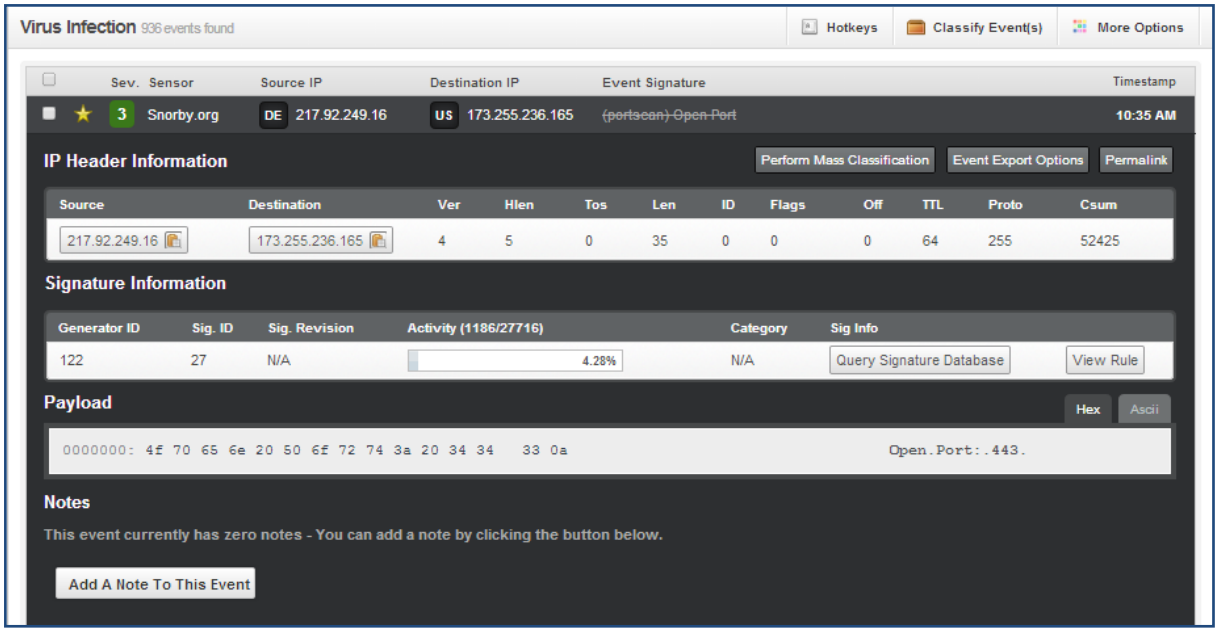

Figura 5.36. Información detallada de un registro del apartado virus infection.
Fuente: http://demo.snorby.org/

O en este otro caso, se trata de un ataque de denegación de servicios, (véase figura 5.37) se puede ver un *payload* que contiene tráfico capturado (cuadro verde) como lo hace la herramienta Wireshark, este tipo de tráfico capturado puede servir para la creación de reglas de Snort y así poder detectarlas en caso de que se presente el mismo ataque, porque ese tipo de tráfico capturado permite conocer el comportamiento de la herramienta que se está utilizando para lanzar el ataque. Tiene dos opciones, ver el *payload* en formato hexadecimal o en formato ASCII.

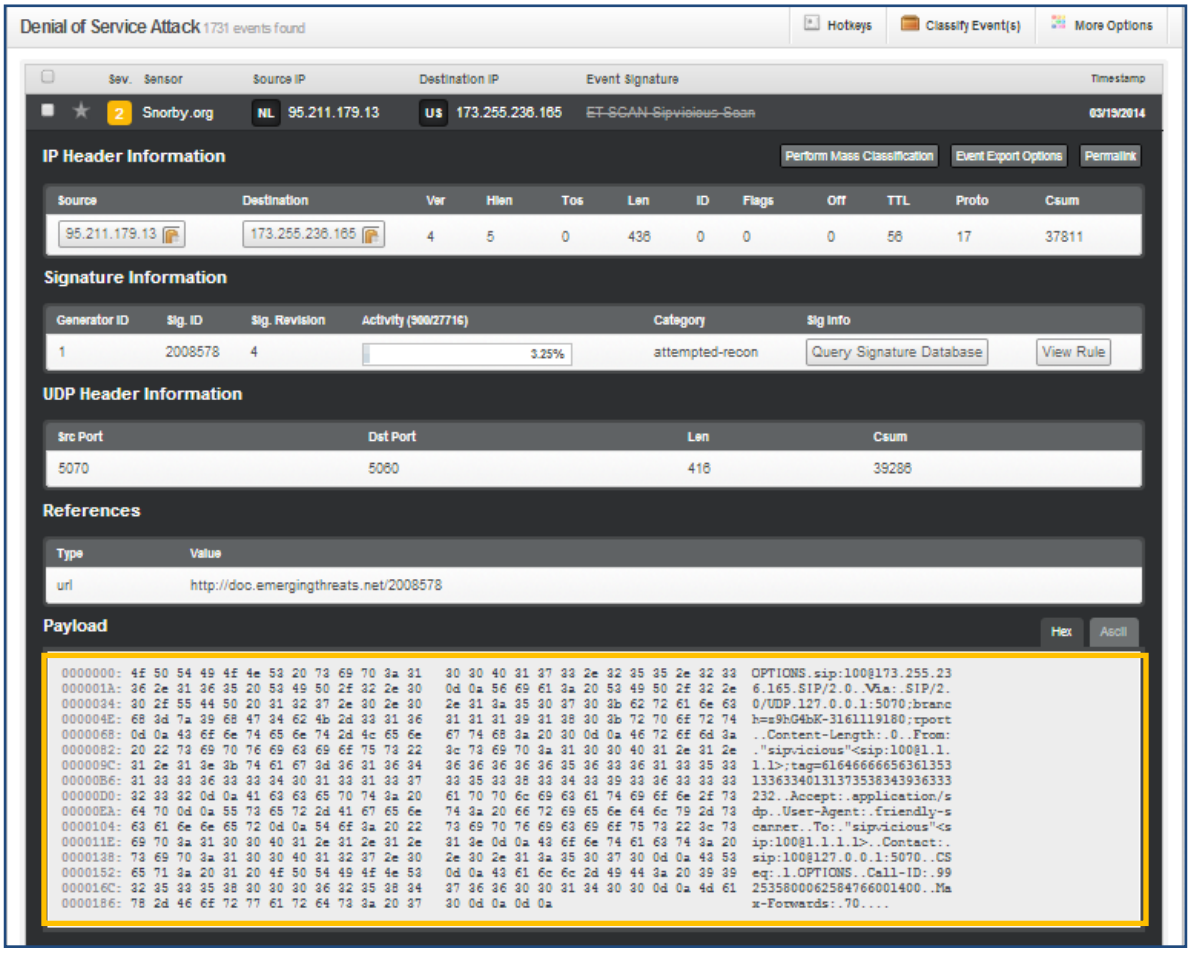

Figura 5.37. Registro de un DoS.
Fuente: http://demo.snorby.org/

Ahora dentro de la sección “administración” se encuentran los ajustes generales como se muestra (véase figura 5.38) Aquí en esta sección se pueden hacer ajustes, por ejemplo, el envío de los reportes con el trafico capturado este puede ser diario, semanal o al mes.

Otro de los ajustes es “address lookups” esta opción permite al analista realizar consultas básicas sobre las direcciones de origen y de destino utilizando fuentes externas.

La opción “enable global event notifications”, muestra la notificación de nuevos eventos globales.

La opción “GeoIP”, muestra información sobre una lista de eventos.

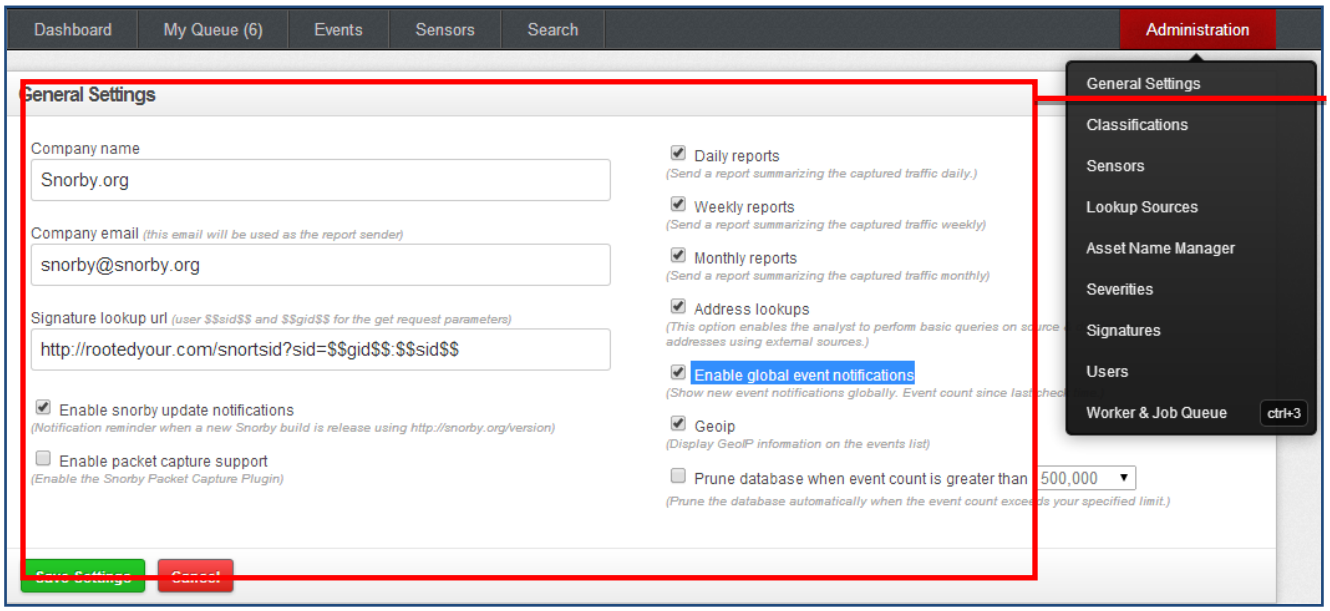

Figura 5.38. Página de ajustes de Snorby.
Fuente: http://demo.snorby.org/

En la parte donde se muestran las gráficas de pastel (véase figura 5.39), dentro de la pestaña de “signatures” se muestra el número total de los eventos (cuadro rojo). A continuación se muestran estos ejemplos.

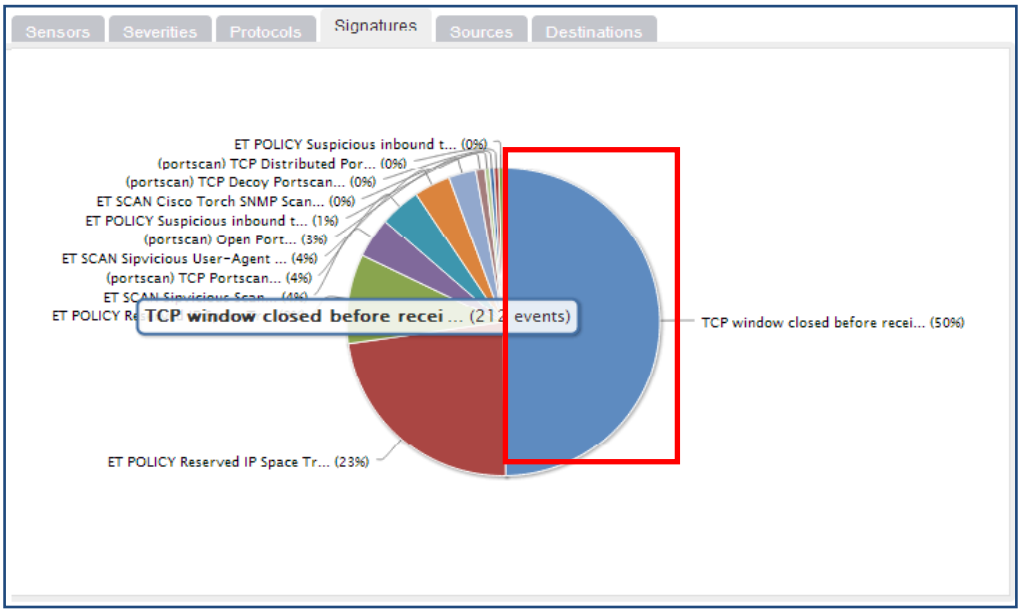

Figura 5.39. Eventos totales TCP cuando se cierra la ventana antes de recibir datos.
Fuente: http://demo.snorby.org/

En la pestaña de “sources” (véase figura 5.40) muestra las IPs así como el número de sesiones de dichas IP, por ejemplo en este caso la IP 106.120.122.131.

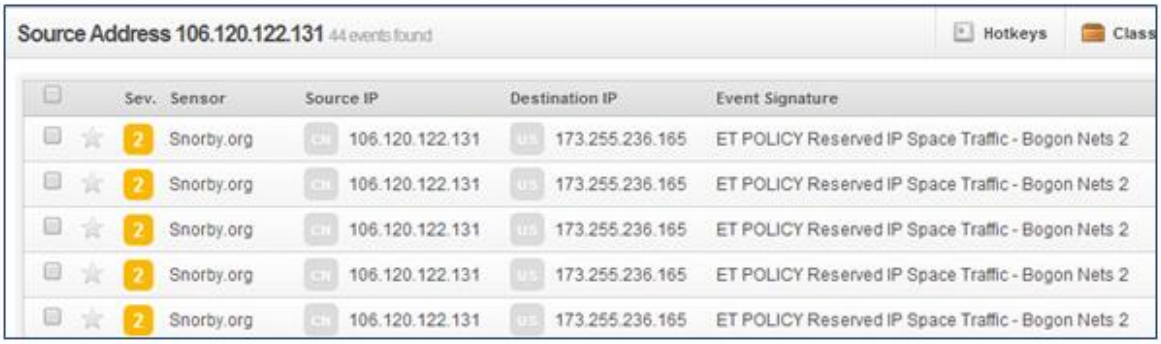

Figura 5.40. IP fuente que realizó este evento hacia una IP destino.
Fuente: http://demo.snorby.org/

Estos serían algunos ejemplos acerca del funcionamiento de Snorby, como se puede apreciar, cuenta con una interfaz muy amigable para el usuario, además de que es fácil interpretar la información que ahí se muestra, todo viene bien especificado y detallado.

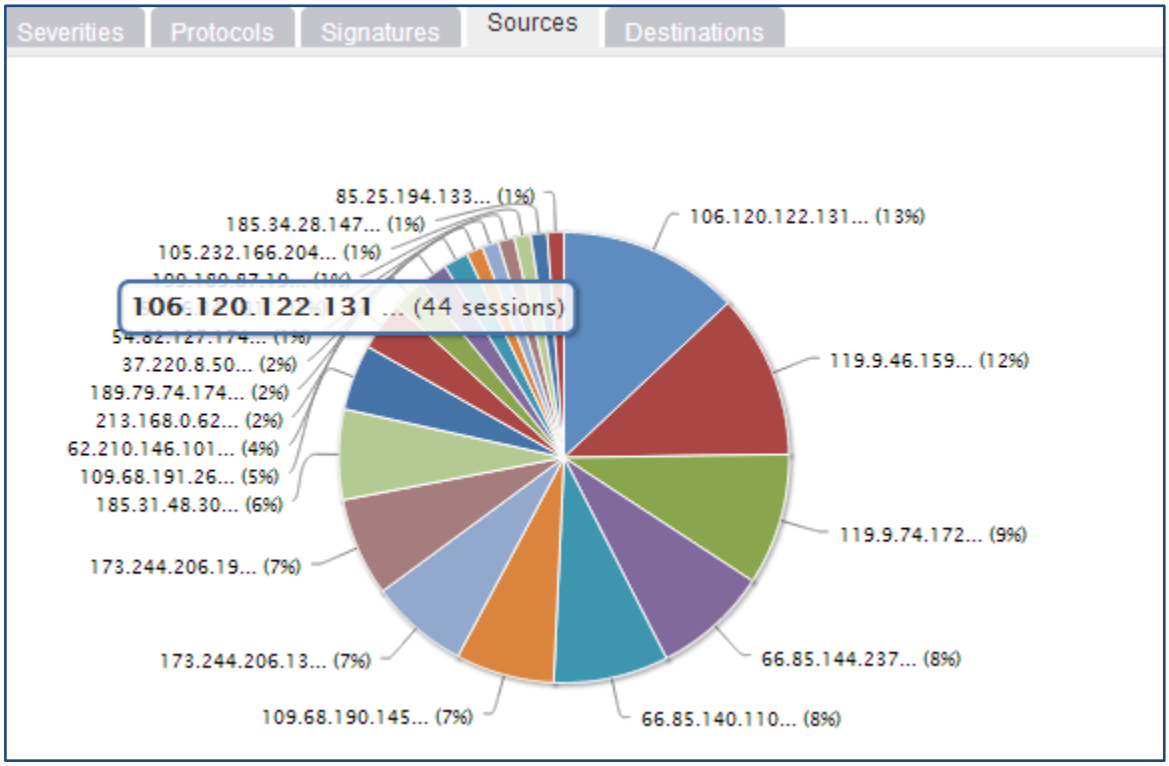

Figura 5.41. La IP 106.120.122.131 realizó 44 sesiones de tipo "ET POLICY Reserved IP Space Traffic - Bogon Nets 2".
Fuente: http://demo.snorby.org/

Además de que muestra el tráfico capturado, que esto puede ser de gran ayuda para la creación de nuevas reglas para Snort y poder así fácilmente contrarrestar el ataque o saber qué hacer en esos casos cuando se presente de nuevo ese ataque.

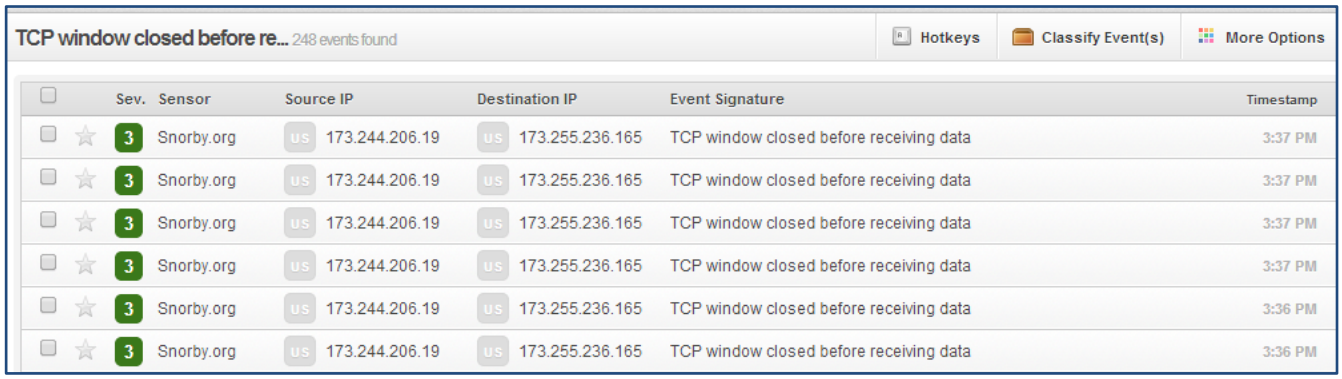

Figura 5.42. Sesiones tipo "ET POLICY Reserved IP Space Traffic - Bogon Nets 2".
Fuente: http://demo.snorby.org/

Otros ejemplos de una gráfica de pastel y de direcciones IP de donde proviene una amenaza, (véase figura 5.41 y 5.42) respectivamente.

Conclusiones

Conclusiones

Se puede concluir que la seguridad es muy importante en todos los ámbitos, como sería la seguridad personal o de una organización, se sabe que la seguridad es un factor para poder prevenir cualquier tipo de acontecimiento, para proporciona bienestar y tranquilidad, enfocándose hacia la seguridad informática se puede decir que es una medida de protección de todos los bienes con los que cuenta una organización .

A través de esta investigación se dieron a conocer algunas de las medidas de protección con las que deberían de contar las organizaciones que manejen información confidencial, como por ejemplo la información que se maneja en instituciones bancarias, como las cuentas de los clientes, direcciones de los clientes, números de tarjeta, por nombrar algunas. Sería un gran problema y riesgo si toda esa información llegara a caer en manos de los ciberdelincuentes o de personas que hagan mal uso de estos bienes.

Durante años se han puesto en práctica muchas medidas de seguridad y no sólo de software, sino también de hardware como por ejemplo algunos sensores biométricos, que permiten el control de acceso a personas que no sean de áreas correspondientes.

Una de las áreas que constituye la seguridad informática es la criptografía[46], sin ella no sería muy seguro realizar algún tipo de compra o transacción por internet, ya que cualquier ciberdelincuente que este a la espera o cazando a su víctima, pueda ver esa información y robarla, como han existido casos en los cuales las personas que están conectadas en una red inalámbrica de un hotel y hacen todo tipo de uso de ésta, un intruso podría ver qué es lo que está realizando su víctima sin que ésta se dé cuenta que alguien la está observando, entonces es ahí donde entra en juego la criptografía y la seguridad.

La criptografía ha existido desde que los egipcios la utilizaban para codificar alguna información o cuando el emperador Julio César enviaba información militar confidencial. En la actualidad se están realizando pruebas con la criptografía cuántica, la cual se basa en leyes de la física gracias a la mecánica cuántica, como el teorema de *no cloning,* el cual dice que cualquier estado cuántico no puede ser copiado, por lo

cual ningún intruso podrá clonar o copiar ese tipo de cifrado a menos que exista una copiadora cuántica, por mencionar un caso.

Como en la actualidad se ha notado más la actividad de esos grupos de ciberdelincuentes, las empresas deberían de tener una mayor y mejor protección para que los activos no sean robados. Este tipo de actividad se ha venido dando por varias cuestiones, la principal causa de este tipo de movimientos o revueltas es por cuestiones políticas, porque a la gran mayoría de estas personas están en desacuerdo con las decisiones que se toman y están en todo su derecho de manifestarse o están inconformes con esas decisiones, pero tampoco está bien que a consecuencia de eso algunas organizaciones sufran ataques de este tipo de personas, que en lugar de usar ese conocimiento para beneficio de muchos, lo utilizan para realizar actos delictivos.

Es por eso que existen personas que también se dedican a realizar ese tipo de pruebas y con esto saber qué tipo de mecanismo de ataque utilizarán los ciberdelincuentes, se tiene que pensar como ellos para así saber cuál será su siguiente movimiento.

Los ciberdelincuentes se aprovechan en muchas ocasiones, del enojo de las personas que tienen hacia cierto personaje político o empresarial, las convocatorias para que se unan a la "causa" por decirlo así son varias, dichas convocatorias salen en las redes sociales como Facebook, Twitter y YouTube, donde se dan las instrucciones o pasos a seguir para que ayuden a realizar un ataque dirigido a una organización gubernamental o financiera, entonces estas personas se unen y descargan una serie de herramientas que les ayudan a realizar ataques desde su computadora, estas herramientas puede ser una aplicación o una página en JavaScript, ésta última se deja abierta y en ese momento empieza a lanzar solicitudes a la página que se quiere atacar, iniciando con esto un ataque de denegación de servicio distribuida (DDoS), que es la preferida por este tipo de organizaciones, como la famosa organización Anonymous.

Es por eso que la seguridad informática se ha vuelto un área fundamental en cualquier organización.

[46] Criptografía: Es la ciencia que se encarga del estudio de técnicas para transformar la información a una forma que no pueda entenderse a simple vista; sin embargo, el objetivo de la Criptografía no es sólo mantener los datos secretos, sino también protegerlos contra modificación y comprobar la fuente de los mismos.

Referencias

Referencias

(s.f.).

(ELSA), E. l. (Abril de 2012). Recuperado el 30 de Diciembre de 2013, de https://code.google.com/p/enterprise-log-search-and-archive/

Adminso. (Junio de 2013). *Instalación y Configuración de Snort*. Recuperado el 01 de Enero de 2014, de http://www.adminso.es/images/0/06/Pfc_Carlos_cap4.pdf

Aldeid. (23 de Noviembre de 2013). *Snorby*. Recuperado el 09 de Enero de 2014, de http://www.aldeid.com/wiki/Snorby

Alfon. (14 de Febrero de 2011). *Seguridad y Redes*. Recuperado el 25 de Noviembre de 2013, de http://seguridadyredes.wordpress.com/2011/02/14/snort-security-onion-live-sguil-squert-y-suricata-todo-en-uno-parte-i/

Aranda, G. (14 de Mayo de 2012). *System Backdoors*. Recuperado el 25 de Noviembre de 2013, de http://systembackdoors.blogspot.mx/2012/05/security-onion-configuracion-basica.html

Bone, A. (Julio de 2013). *RT for Incident Response .* Recuperado el 31 de Enero de 2014, de http://www.terena.org/activities/tf-csirt/meeting9/bone-rtir.pdf

Burks, D. (14 de Noviembre de 2013). *Security Onion*. Recuperado el 25 de Noviembre de 2013, de https://code.google.com/p/security-onion/wiki/Installation

Burks, D. (Noviembre de 2013). *Security Onion*. Recuperado el 25 de Noviembre de 2013, de http://blog.securityonion.net/p/securityonion.html

Camacho, D. J. (Junio de 2012). *Herramientas Para la Búsqueda Virtual en Internet*. Recuperado el 22 de Octubre de 2013, de http://www.uv.mx/jdiaz/combas/tareas/modulo2/pdf/Contenido%202.2.2%20-R3Z%20y%20M.pdf

Chicago, U. o. (06 de Noviembre de 2012). *Request Tracker (RT)*. Recuperado el 31 de Enero de 2014, de http://accc.uic.edu/service/rt

Cisco. (Noviembre de 2004). *IPS External*. Recuperado el 01 de Enero de 2014, de http://www.cisco.com/web/LA/productos/servicios/docs/IPS_external_qa_clients_Spanish.pdf

CSIRT, J. (Enero de 2014). *RTIR incident handling .* Recuperado el 16 de Enero de 2014, de http://www.bestpractical.com/static/rtir/janet-workflow.pdf

Davis, H. (2006). *Search Engine Optimization.* O' Reilly.

Devjoker. (04 de Junio de 2007). *¿Cómo crear RSS?* Recuperado el 12 de Marzo de 2014, de http://www.devjoker.com/print/Tutorial-RSS/270/Tutorial-RSS.aspx

ESLARED. (Junio de 2012). *Instalación y Configuración de Request Tracker (RT) .* Recuperado el 18 de Marzo de 2014, de http://www.eslared.org.ve/walc2012/material/track3/rt-lab-1.pdf

Falcone, K. (Agosto de 2013). *Terena.* Recuperado el 16 de Enero de 2014, de http://www.terena.org/activities/tf-csirt/meeting38/falcone-rtir.pdf

Fernández, A. R. (Junio de 2013). *Universidad Politecnica de Catalunya*. Recuperado el 06 de Enero de 2014, de http://docencia.ac.upc.es/FIB/CASO/seminaris/2q0304/M6.pdf

GitHub. (Abril de 2013). *Squert*. Recuperado el 04 de Diciembre de 2013, de https://github.com/int13h/squert

Gupta, S. (2012). *Logging and Monitoring to Detect Network.*

Hackers, D. (08 de Octubre de 2012). *Nmap: escáner de puertos*. Recuperado el 25 de Marzo de 2014, de http://www.debianhackers.net/nmap-escaner-de-puertos

Hacking, F. a. (Febrero de 2014). *Armitage*. Recuperado el 25 de Marzo de 2014, de http://www.fastandeasyhacking.com/manual

Halliday, P. (Noviembre de 2013). *GitHub*. Recuperado el 04 de Diciembre de 2013, de https://github.com/int13h/squert

Henriques, T. (14 de Febrero de 2013). *How to Install and Use Security Onion*. Recuperado el 04 de Diciembre de 2013, de http://ptcoresec.eu/2013/02/14/tutorial-how-to-install-and-use-security-onion-pt-1/

Informática, I. (08 de Agosto de 2013). *Seguridad Informática y de la Información*. Recuperado el 25 de Marzo de 2014, de http://www.inseguridadinformatica.com/2013/08/como-instalar-el-armitage-en-kali-linux.html

Institute, S. (04 de Julio de 2012). Logging and Monitoring to Detect Network Intrusions and Compliance Violations in the Environment.

Janet. (Enero de 2014). *Computer Security and Incident Response Team (CSIRT).* Recuperado el 16 de Enero de 2014, de https://www.ja.net/products-services/janet-connect/csirt?

Kioskea. (Diciembre de 2013). *Sistema de Detección de Intrusiones IDS*. Recuperado el 01 de Enero de 2014, de http://es.kioskea.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

Kioskea. (Marzo de 2014). *Protocolo ICMP*. Recuperado el 13 de Marzo de 2014, de http://es.kioskea.net/contents/265-el-protocolo-icmp

Kioskea. (Marzo de 2014). *Traceroute*. Recuperado el 13 de Marzo de 2014, de http://es.kioskea.net/contents/357-traceroute

Leune, K. (21 de Febrero de 2009). *Application for Incident Response Teams (AIRT)*. Recuperado el 16 de Enero de 2014, de http://airt.leune.com/

Madrid, P. B. (Abril de 2011). *Sistemas y Motores Busqueda.* Recuperado el 23 de Octubre de 2013, de www.ucol.mx/despacho/diplomado/SistemasyMotoresBusqueda.ppt?

McRee, R. (Agosto de 2009). *Holistic Infosec.* Recuperado el 16 de Enero de 2014, de http://holisticinfosec.org/toolsmith/pdf/august2009.pdf

Moorhy, S. (06 de Agosto de 2010). *The Geek Stuff*. Recuperado el 06 de Enero de 2014, de http://s3.amazonaws.com/snort-org/www/assets/219/snort2953_fedora.pdf

MySQL. (Febrero de 2011). *Información General*. Recuperado el 03 de Noviembre de 2013, de http://dev.mysql.com/doc/refman/5.0/es/introduction.html

MySQL. (Febrero de 2011). *Panorámica del Sistema de Gestión de Base de Datos MySQL*. Recuperado el 03 de Noviembre de 2013, de http://dev.mysql.com/doc/refman/5.0/es/what-is.html

Nmap. (Mayo de 2013). *Nmap Security Scanner*. Recuperado el 25 de Marzo de 2014, de http://nmap.org/

NorfiPC. (Abril de 2013). *Como crear un archivo de fuentes de noticias o feed RSS para un sitio web*. Recuperado el 12 de Marzo de 2014, de http://norfipc.com/web/como-hacer-archivo-fuentes-noticias-feed-rss.html

OpenFPC. (Enero de 2014). *Full Packet Capture*. Recuperado el 09 de Enero de 2014, de http://www.openfpc.org/

OSIATIS. (Enero de 2014). *Gestión de Incidentes*. Recuperado el 16 de Enero de 2014, de http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/vision_general_gestion_de_incidentes/vision_general_gestion_de_incidentes.php

PHP. (Marzo de 2013). *Controladores y Complementos de MySQL*. Recuperado el 06 de Noviembre de 2013, de http://www.php.net/manual/es/set.mysqlinfo.php

Practical, B. (Enero de 2014). *Request Tracker*. Recuperado el 16 de Enero de 2014, de http://www.bestpractical.com/rt/docs.html

Project, S. (Abril de 2012). *Squert*. Recuperado el 04 de Diciembre de 2013, de http://www.squertproject.org/

Project, S. (Mayo de 2013). *Squert*. Recuperado el 04 de Diciembre de 2013, de http://www.squertproject.org/

PTCoreSec. (14 de Febrero de 2013). *Tutorial: How to install and use Security Onion (Pt. 1)*. Recuperado el 04 de Diciembre de 2013, de http://ptcoresec.eu/2013/02/14/tutorial-how-to-install-and-use-security-onion-pt-1/

Rich, A. (Octubre de 2005). *Oracle*. Recuperado el 07 de Enero de 2014, de http://www.oracle.com/technetwork/systems/articles/snort-base-jsp-138895.html#intro

Riley, C. (Marzo de 2013). *Seguridad Snort*. Recuperado el 01 de Enero de 2014, de http://www.linux-magazine.es/issue/46/060-066SnortLM46.pdf

Robots Txt. (2007). Recuperado el 23 de Octubre de 2013, de http://www.robotstxt.org/

Security, E. U. (Enero de 2014). *AIRT (Application for Incident Response Teams)*. Recuperado el 16 de Enero de 2014, de https://www.enisa.europa.eu/activities/cert/support/chiht/tools/airt-application-for-incident-response-teams

Security, E. U. (Enero de 2014). *RTIR (Request Tracker for Incident Response)*. Recuperado el 16 de Enero de 2014, de http://www.enisa.europa.eu/activities/cert/support/chiht/tools/rtir-request-tracker-for-incident-response

Sinemed. (Abril de 2011). *¿Qué es MySQL?* Recuperado el 03 de Noviembre de 2013, de http://www.sinemed.com/recursos/docs/MySQL.pdf

Snort. (Marzo de 2013). *About Snort*. Recuperado el 30 de Diciembre de 2013, de http://www.snort.org/

Snort. (29 de Mayo de 2013). *Snort User Manual*. Recuperado el 30 de Diciembre de 2013, de http://s3.amazonaws.com/snort-org/www/assets/166/snort_manual.pdf

Sorceforge. (Junio de 2013). *Sguil*. Recuperado el 04 de Diciembre de 2013, de http://sguil.sourceforge.net/index.html

Taringa. (Noviembre de 2013). *Pentesting con Kali Linux Parte IV*. Recuperado el 25 de Marzo de 2014, de http://www.taringa.net/posts/linux/16952716/Pentesting-con-Kali-Linux-Parte-IV.html

Tilburg, U. v. (Diciembre de 2009). *Application for Incident Response Teams.* Recuperado el 16 de Enero de 2014, de http://www.terena.org/activities/tf-csirt/meeting16/airt-nijssen.pdf

Torres, D. (Abril de 2012). *Sistema de Detección de Intrusos*. Recuperado el 01 de Enero de 2014, de http://seguridadinformaticaufps.wikispaces.com/file/view/1150214.pdf

Vicente, C. (Mayo de 2008). *Sistemas de Manejo de Incidencias.* Recuperado el 18 de Marzo de 2014, de https://nsrc.org/workshops/2008/walc/presentaciones/RT.pdf

Visscher, B. (Julio de 2007). *Sguil*. Recuperado el 04 de Diciembre de 2013, de http://sguil.sourceforge.net/index.html

Wikia. (Enero de 2014). *Request Tracker Wiki*. Recuperado el 16 de Enero de 2014, de http://requesttracker.wikia.com/wiki/HomePage

WordPress. (01 de Diciembre de 2010). *Seguridad y Redes*. Recuperado el 09 de Enero de 2014, de http://seguridadyredes.wordpress.com/2010/12/01/snort-snorby-un-front-end-para-analisis-y-gestian-de-alertas-para-snort/