Universidad de las Ciencias Informáticas

Facultad # 2

Título: “Propuesta para la Recolección Centralizada de Logs”

Trabajo de Diploma para optar por el título de
Ingeniero en Ciencias Informáticas

Autor(es): Osmani López Cardoso.

Alexey García Arévalo.

Tutor(es): Ing. Luis Orlando Martin Álvarez.

Ing. Leosdany Sánchez Alba.

Ciudad de la Habana, Junio de 2008.

Año 50 de la Revolución.

En lugar de ser un hombre de éxito, busca ser un hombre valioso: lo demás llegará naturalmente.

Albert Einstein

DECLARACIÓN DE AUTORÍA

Declaramos ser autores de la presente tesis y reconocemos a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo.

Para que así conste firmo la presente a los 27 días del mes de Junio del año 2008.

Osmani López Cardoso, Alexey García Arévalo

_____ _____

Firma del Autor Firma del Tutor

DATOS DE CONTACTO

Tutor: Ing. Luis Orlando Martin Álvarez. Graduado de Ingeniero en Ciencias Informáticas en el curso 2006-2007 en la Universidad de las Ciencias Informáticas. Actualmente trabaja en el departamento de Seguridad Informática de la Universidad de las Ciencias Informáticas.
Correo electrónico: lmartin@uci.cu

Co-tutor: Ing. Leosdany Sánchez Alba. Graduado de Ingeniero en Ciencias Informáticas en el curso 2006-2007 en la Universidad de las Ciencias Informáticas. Actualmente trabaja en el Polo de Seguridad Informática de la universidad. Es profesor de Matemática.
Correo electrónico: lsancheza@uci.cu

AGRADECIMIENTOS

Durante todos mis años de estudios y aun estando tan lejos me guiaron todos estos años. Por ello el mayor agradecimiento es para mis padres.

A mi novia por entenderme y aun pasando tantas horas sin vernos por el tiempo dedicado a este trabajo siempre estuvo a mi lado para ayudarme y quererme.

A todos los integrantes de la comunidad de software libre que nos ayudaron: Kike, El Hacker, Ludwing, Iván, Camilo, Yanio, Vladimir, entre otros que con sus conocimientos de Linux ayudaron mucho durante todo este tiempo.

A la comunidad.

A nuestro tutor Luis Orlando Martín Álvarez.

A nuestro cotutor Leosdany Sánchez Alba por su gran ayuda en la revisión del documento.

A los trabajadores del departamento de Seguridad Informática.

Y a todos aquellos que al menos preguntaban “y la tesis qué”.

Alexey

Quiero dar gracias a Dios por la tesis que hemos desarrollado mi compañero de aula Alexey García Arévalo y yo, aunque en ocasiones pensamos que no podíamos terminar a tiempo nunca nos dimos por vencido. Agradecimientos a mi Familia en Villa Clara, en especial a mi mamá y a mi futura esposa que siempre me apoyaron en todo lo que estaba a su alcance. Quiero dar gracias a todos los “Linuceros” del laboratorio 301 quienes nos brindaron su apoyo incondicional, agradecimientos especiales a Jorge Luis, Yanio, Ludwing, Kike, Camilo, Ivan. Quiero agradecer a nuestros tutores Ing. Luis Orlando Martin Álvarez e Ing. Leosdany Sánchez Alba por la ayuda que nos brindaron durante el desarrollo de la tesis. Agradecimientos a todos aquellos que de una forma u otra nos ayudaron.

Osmani

DEDICATORIA

A mis padres que siempre han sido guía en todos mis años de estudios.

A mi familia y amigos que hicieron posible este trabajo.

A los que cada día trabajan por el bienestar de los demás y construyen un futuro mejor.

Alexey.

A mi Familia que siempre me han apoyado durante mi carrera en la UCI.

A mi mamá y a mi futura esposa.

A todos aquellos que de una forma u otra han tenido que ver con esta tesis.

Osmani.

RESUMEN

Para mantener la seguridad de una red existen muchas herramientas que permiten a los administradores detectar posibles acciones malignas. Los logs que se generan en las computadoras y servidores son una fuente muy importante de información a tener en cuenta. En una computadora se producen eventos que generan logs ya sea por la acción de algún usuario o por el propio sistema. Es importante que dentro de una red sean recopilados todos estos eventos centralizadamente para su posterior procesamiento.

En la UCI no se realiza la recolección centralizada y sistemática de los registros de eventos generados en las computadoras de su red y algunos servidores, perdiéndose así un gran volumen de información importante que puede ser procesada con el objetivo de detectar posibles acciones malignas. Por ello se hace necesario instalar un sistema que sea capaz de recopilar los logs de las computadoras y servidores de determinadas áreas en un servidor central. La presente investigación se propone darle solución a esta situación. Para ello se llevó a cabo una profunda investigación acerca de los sistemas existentes para la recolección de logs que fueran libres. Luego se instalaron y probaron estos sistemas para determinar así finalmente el más indicado para aplicar en la UCI.

PALABRAS CLAVE

Seguridad

Logs

Evento

Recolección

Centralizada

TABLA DE CONTENIDOS

INTRODUCCIÓN

Para el buen funcionamiento y hacer un uso óptimo de una red así como de cada una de las computadoras y dispositivos que conforman la misma se hace necesario mantener buenas políticas de seguridad con el objetivo de impedir que ocurran acciones que vayan en contra de la ética informática, como pueden ser el robo de contraseñas o claves, eliminación, apropiación o modificación de información sensible, acceso a lugares restringidos, etc. Para no ser afectados por ninguna de estas acciones es que debemos utilizar todo lo que esté al alcance, ya sean herramientas externas o utilizando las que ya brindan las propias PC (del inglés Personal Computer o Computadora Personal).

Entre las cosas que están al alcance y que pueden ser utilizadas están los “Logs”. Desde que un usuario se loguea hasta que cierre la sesión en una computadora se almacena información, a modo de historial, acerca de todas las acciones realizadas mientras la sesión estuvo abierta, incluyendo todas las aplicaciones abiertas, errores ocurridos, accesos al sistema, el tráfico capturado por un sniffer, mensajes de información del kernel, cambio de privilegios a alguna cuenta de usuario, etc. A dicho historial realizado por la propia PC es a lo que se le conoce como Logs, aunque también se les conoce como Registro de Eventos o Eventos propiamente en otros casos.

Los eventos son elementos muy importantes y son una fuente de información a tener en cuenta para la administración y seguridad de redes, ya que luego de haber ocurrido alguna violación en la red o acción indebida, se les puede realizar un análisis para identificar datos imprescindibles como el autor, desde qué computadora se cometió la violación, la hora y el día, entre otros que ayudarán a esclarecer el hecho. Gracias a la información almacenada en los logs es que se puede tener pruebas de cualquier violación que se halla cometido en una determinada red o incluso en una única computadora, por lo que puede ser usada perfectamente como evidencia digital ante la ley. La evidencia digital constituye una prueba física que está construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales. (Giovanni Zuccardi, 2006)

Para el análisis de los logs de toda una red debe existir previamente un sistema que sea capaz de recopilar todos los registros de eventos ocurridos de todas las computadoras conectadas a esta. Es importante tener en cuenta que en una red pueden existir computadoras con sistemas operativos diferentes y se ejecutan programas que generan sus propios eventos. Un sistema recolector de logs debe ser capaz de, independientemente del sistema operativo donde trabaje, pueda recoger los logs

de todas las computadoras, para ello en su mayoría los logs son almacenados en un formato estándar, así cualquier registros de evento ocurrido en algún dispositivo puede ser leído y procesado por otros.

La recolección se debe realizar en tiempo real y sistemáticamente. Esto quiere decir que en la medida en que se van generando los logs deben ser recogidos hacia un servidor central, permitiendo que se tenga la información más fresca y actual de la ocurrencia de cualquier hecho indebido o algún error.

Situación Problémica.

En la Universidad de las Ciencias Informáticas (UCI) no se recogen los logs de eventos generados por las computadoras de su red de forma centralizada, tampoco se hace sistemáticamente ni en tiempo real. Actualmente se pierde mucha información que puede ser muy importante para la detección de incidencias negativas. Para el departamento de Seguridad Informática de la universidad le resulta muy necesario recopilar centralmente los logs generados en un grupo de computadoras, que trabajan tanto en Linux como en Windows, y servidores que son vitales para el desarrollo de la docencia y el uso eficiente de la red. A las áreas donde se encuentran estas computadoras se determinó nombrarles como Áreas de Riesgo. Después de un análisis exhaustivo se llegó a la conclusión de que el **problema a resolver** era: ¿Cómo recopilar los logs de las máquinas de las Áreas de Riesgo de la red de la UCI de forma centralizada y sistemática? De ahí que como **objeto de estudio** de la investigación se definió: las herramientas libres existentes en el mundo que sean capaces de recopilar los datos contenidos en los registros de eventos en un servidor central, teniendo así como **campo de acción**: los logs generados por las computadoras de las áreas de Laboratorios de Docencia, aulas así como los de los servidores de Squid y el Controlador de Dominio o Áreas de Riesgo. A partir del problema planteado se define como **objetivo general**: encontrar un sistema capaz de recopilar los logs de eventos de las computadoras de las Áreas de Riesgo con la característica de ser libre de costo monetario y de código abierto.

Para lograr el cumplimiento del **objetivo general** se determinó el siguiente conjunto de **objetivos específicos**:

- Adquirir información sobre el tema relacionado con los logs.
- Hacer una búsqueda de las distintas herramientas existentes para la recolección de eventos y que cumplan con la condición de ser libres de costo y de código abierto.
- Verificar el funcionamiento de las herramientas encontradas para la recolección de eventos.

- Definir el sistema que se aplicaría en la UCI.

Y para darle solución a los objetivos planteados se formularon una serie de orientaciones concretas o **tareas investigativas** que sirvieron de apoyo. Las mismas fueron:

- Investigar todo lo que se ha hecho en el mundo en cuanto a la recolección centralizada de logs.
- Resumir el análisis de la documentación relacionada con el objeto de estudio en la UCI, en Cuba y en el resto del mundo.
- Entrevistar a los administradores de red de la UCI.
- Adquirir conocimiento de las distribuciones del sistema operativo Linux, donde se instalarán las distintas herramientas de gestión de logs existentes para observar su funcionamiento.
- Instalar y configurar los sistemas encontrados.

Beneficios del sistema.

El Sistema de Recolección Centralizada de los Logs reportará muchos beneficios tanto para la seguridad de la universidad como para los encargados de administrar la red. Para la seguridad porque permitirá recopilar toda la información de los eventos ocurridos en las computadoras de las Áreas de Riesgo con el objetivo de obtener todos los datos de posibles violaciones de seguridad, errores ocurridos, etc. Y para los administradores porque humanizará el trabajo ya que anteriormente no se hacía centralizadamente el trabajo con los logs, ni se tenía una sistematicidad en esto, teniendo muchas veces que trabajar con volúmenes muy grandes de información, que se acumulaban precisamente por no realizar un trabajo continuo con los logs, ahora se hará el trabajo más fácil ya que automáticamente se encargará de ir registrando y archivando toda la información obtenida de los registros de eventos de las computadoras. Así los administradores podrán acceder a los datos registrados en un intervalo de tiempo deseado en el que ocurrió una determinada violación, no teniendo que buscar en un volumen de información mucho más grande. Además de esto garantizará que la información se procese con mayor rapidez, por lo que cualquier modificación que ocurra será reportada inmediatamente, teniendo mayor fiabilidad para ser utilizada como prueba judicial de la ocurrencia del hecho que le dio origen.

Otro factor muy importante es que un sistema con las características de que todos sus componentes sean libres permitirá a la UCI no realizar grandes gastos monetarios para adquirirlo. Actualmente los precios de los software para la recolección de eventos que son propietarios son muy variables, los más

baratos cuestan varios miles de dólares, incluso algunos llegando a varias decenas de miles. El hecho de que un software sea propietario significa que además del costo monetario por adquirirlo, los usuarios no tienen acceso al código fuente del programa por lo que no pueden modificarlo. El precio que tengan estas herramientas muchas veces depende de la cantidad de computadoras de las que se recogerán los logs. Teniendo en cuenta que la red de la UCI es muy grande, evidentemente el valor a pagar sería mucho mayor por este concepto.

Diseño metodológico

Métodos Teóricos

- Método Sistémico: se utilizó este método para la determinación de los componentes que conforman una buena recolección de logs, así como la relación que existe entre ellos, determinando la estructura y la jerarquía existente entre dichos componentes.
- Analítico-Sintético: luego de una investigación acerca del tema, del estado del arte a nivel mundial y más específicamente en la propia Universidad de Las Ciencias Informáticas, se sintetizó toda la información que se consideró importante para el desarrollo del trabajo.

Métodos Empíricos

- Método de la Medición: fue necesario utilizar este método para medir numéricamente el volumen de información que se genera en una porción de la red de la universidad.
- Método de la Entrevista: se entrevistó al cliente con el objetivo de obtener información acerca de que era lo que necesitaba y las características que debería tener el sistema.

Antecedentes de este trabajo:

Actualmente la mayoría de los dispositivos, equipos y herramientas utilizados en las redes generan ficheros logs, desde firewall, antivirus, aplicaciones, etc. Se han desarrollados proyectos para la recolección y análisis de estos eventos dada la importancia que tienen para la seguridad del entorno. En la UCI en cierta medida se recopilan los logs de las computadoras pero no centralizadamente, sino que se recogen eventos de determinadas porciones de la red en caso de alguna violación. Hay que destacar que muchas veces porciones de información por separado no muestran determinados elementos que son importantes y eso ocurre en estos casos también. Además, no se hace un trabajo sistemático, o sea, no se hace continuamente el registro de los logs, sino que cuando ocurre alguna acción negativa es cuando se busca, dentro de un gran volumen de información acumulada, el origen

de la violación. La falta de un trabajo sistemático es un problema muy grande teniendo en cuenta que en cada computadora se genera un gran número de logs debido a que están siendo utilizadas casi todo el día, son muchos los usuarios que realizan determinadas tareas en ellas, ya sean estudiantes como trabajadores, lo cual indudablemente incide en que se genere un gran volumen de información y si no se recopila continuamente ese volumen será inmenso a la hora de procesarlo.

Existen sistemas que realizan todas las tareas de la recolección de los registros de eventos de forma centralizada, donde la arquitectura principal que se sigue es la de cliente-servidor. A través de esta arquitectura las aplicaciones clientes que se instalarán en cada una de las computadoras de la red envían constantemente información de los logs a la aplicación servidor lo cual facilita el procesamiento de la información en caso de que ocurra una determinada violación de la seguridad.

El presente trabajo cuenta con una Introducción general, tres capítulos, Conclusiones de la investigación, Referencias Bibliográficas y Bibliografía así como Anexos.

Capítulo 1.

En el Capítulo 1 se describe el estado actual del trabajo con los logs. Para ello se dan algunos conceptos importantes, se describen protocolos que son usados en la transmisión de eventos a través de la red así como algunas de las herramientas más conocidas en la recopilación de logs.

Capítulo 2.

El Capítulo 2 brinda una descripción profunda de las herramientas que cuentan con rasgos importantes por lo que pueden ser tomadas en cuenta para darle solución al problema planteado. Luego se describen posibles soluciones a través de la integración de algunas de estas para finalmente llegar a la solución escogida.

Capítulo 3.

El Capitulo 3 contiene la descripción de la instalación y configuración de las herramientas que componen la solución determinada en el Capítulo 2.

CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA

1.1 Introducción

En este capítulo se hará una descripción sobre el trabajo que se ha hecho en el mundo con respecto a la recolección centralizada de logs. Existen algunos protocolos que son usados para el trabajo con los eventos de los cuales se hará una breve descripción. A nivel mundial existen muchas herramientas que realizan las tareas de recolección de logs, en Cuba se han llevado a cabo algunos trabajos sobre el objeto de estudio y en el caso de la UCI no se ha desarrollado ningún proyecto en este sentido. Se han creado algunas normas y criterios a tener en cuenta a la hora de trabajar con los eventos. Sobre todo lo antes planteado en este capítulo se profundizará.

1.2 Situación actual de la recolección de logs en el mundo, Cuba y la UCI.

1.2.1 En el mundo.

A nivel mundial se ha trabajado mucho en la centralización de los logs. Se han desarrollado muchas herramientas con gran potencia y velocidad de procesamiento, capaces de recoger los logs y además a partir de la información que contienen realizar reportes y gráficas de los datos recolectados, todo lo cual se hace en tiempo real. Por otro lado en Cuba existe alguna experiencia de trabajos anteriores, algunas instituciones han desarrollado mecanismos para la gestión de los logs. Sin embargo en la UCI aunque no se ha trabajado prácticamente nada se ha comenzado a dar la atención que lleva recopilar los eventos, por la importancia que tienen para la seguridad de la red.

Los logs pueden ser de texto plano ó binario, y son guardados por defecto en un determinado lugar del sistema, pudiéndose hacer uso de ellos e incluso definirles otra localización para su almacenamiento. Los de texto plano están compuestos únicamente por texto sin formato, solo caracteres alfanuméricos (letras y números). Mientras que los de texto binario contienen información de cualquier tipo, codificada en forma binaria (a través de ceros y unos) para el propósito de almacenamiento y procesamiento de computadora.

1.2.1.1 Formato de un log.

Cada línea del archivo de log está configurada con un formato de columnas de este tipo: HOST USERNAME GROUP DATE+TIME OP1 OP2 OP3 OP4 donde:

HOST: la dirección IP origen del usuario que se ha conectado al servidor.

USERNAME: el nombre de usuario que ha escogido la persona que se ha conectado al servidor.

GROUP: el grupo al que pertenece la persona que se ha conectado al servidor.

DATE+TIME: con el formato YYYY/MM/DD:HH:MM:SS que corresponde a la hora/fecha de entrada en el servidor.

OP1 (Opción/Valor Opcional 1): puede ser uno de los siguientes:

- l: si está este valor entonces OP2 significa que el login ha tenido éxito o ha fallado. OP3 and OP4 no tienen utilidad.
- r: si está este valor entonces OP2 es la ruta del archivo al que se está accediendo, OP3 es el tamaño del archivo en bytes y OP4 es la velocidad de transferencia en k/s.
- w: si está este valor entonces OP2 es la ruta del archivo al que se está accediendo, OP3 es el tamaño del archivo en bytes y OP4 es la velocidad de transferencia en k/s.
- e: si está este valor entonces OP2 es el motivo del error. OP3 and OP4 no tienen utilidad. (Raiden, 2008)

1.2.1.2 Tipos de logs.

Es importante saber que existe un gran número de tipos de logs, muchos por su nombre son propios de determinados sistemas operativos, entre los más conocidos están los correspondientes al Sistema, Aplicaciones y Seguridad que son nativos del sistema operativo Windows, donde a los registros de eventos se les conoce como EventLogs, mientras que los del Kernel corresponden a los sistemas operativos UNIX. En UNIX los eventos se les conocen como Mensajes Syslog debido al protocolo o programa de mismo nombre que traen estos sistemas operativos para la monitorización de los sucesos ocurridos en el sistema. Otros tipos de logs son:

- Del Kernel: los que son del núcleo.
- De Correo: generados por los servidores de correo.
- De Web: son generados por los servidores web a partir de los accesos de los usuarios a sus sitios.
- De Squid: los servidores proxy generan logs sobre todo el tráfico a través de ellos.
- Y otros.

1.2.1.3 ¿Qué es el registro de logs de eventos?

Básicamente el registro de eventos logs es la recolección, monitoreo, análisis y archivado de los logs generados por el sistema o aplicaciones. Una vez que toda la información es concentrada en el servidor se realizan filtrados, auditorias, consultas, se envían alertas a partir del tipo de evento que ocurra. La siguiente figura muestra el evento generado en el Registro de Eventos de Seguridad de Windows cuando se ejecuta la herramienta “Paint” en Windows.

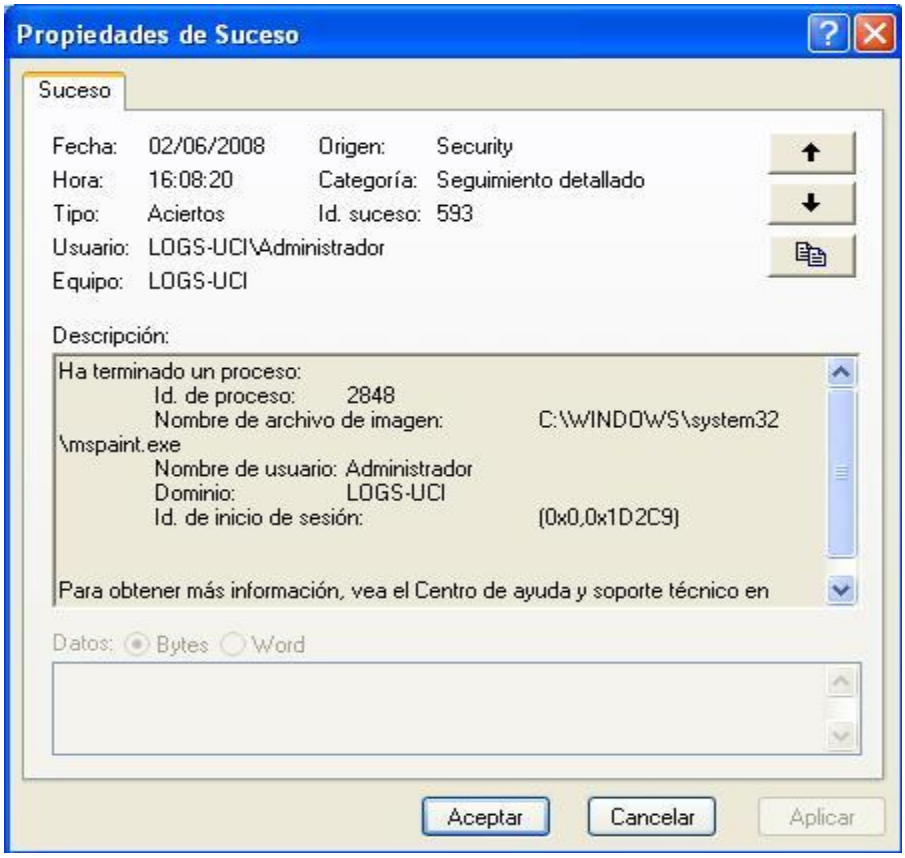

Figura 1. Evento generado al ejecutar el Paint de Windows.

1.2.1.4 ¿Por qué es necesaria la centralización de los logs?

A través de un buen mecanismo de centralización de logs, donde todos los eventos ocurridos en las máquinas estén concentrados y a disposición de los administradores de la red, permitirá realizar mejores análisis y auditorias a los datos. Además dificultará a los posibles atacantes la alteración o borrando de los registros de los ataques efectuados.

CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA.

En la actualidad se emplean muchos recursos en lograr la seguridad máxima en muchas empresas e incluso en sus propios hogares. Se cuentan con muchas herramientas para ello como pueden ser los firewalls, Sistemas de Detección de Intrusos o IDS, antivirus, etc. Dichas herramientas son capaces de vigilar y controlar mucha de la información que se mueve dentro o fuera de la red. Pero con estas acciones no basta, muchas veces ocurren determinados hechos que no pueden ser detectadas. En muchos casos los firewalls, antivirus, etc., no protegen los sistemas de los incidentes negativos que puedan ocurrir dentro de la propia red. Debido a que el trabajo de estas herramientas es por separado, no se logra la eficiencia necesaria. Así en muchos casos se hace necesario hacer un trabajo centralizado con el objetivo de establecer correlaciones entre hechos que brinden mucha más información que por separado. Una solución puede ser la recolección centralizada de los logs, con la que hasta se pueden incluso evitar hechos antes de que ocurran, que pueden traer pérdidas irremediables de información.

Una investigación mostró que el 44% de las empresas no realizan administración de registros de sucesos, principalmente debido al gran volumen de datos a administrar así como a la naturaleza críptica de la información contenida en ellos, como principales razones. Estos desafíos a menudo llevan a que los registros de sucesos no sean administrados, sean infrautilizados e ignorados – hasta que llega el desastre. Los sucesos constituyen una inestimable fuente de información, respondiendo preguntas clave sobre brechas de seguridad, estado de salud de la infraestructura de TI (Tecnologías de la Información), cumplimiento legal e investigación forense. (GFI, 2008)

Luego de una profunda y exhaustiva investigación se comprobó que se ha trabajado bastante a nivel mundial en lo que a la centralización de los logs se refiere. Se comprobó que se han desarrollado muchos sistemas que realizan las acciones de recopilar y procesar registros de eventos, pero que en su gran mayoría son privativos, y que de otros solo es libre una parte de ellos. Partiendo de que la arquitectura principal que se sigue a la hora de desarrollar un software con esta finalidad es la de cliente-servidor, donde en cada computadora una aplicación cliente se encarga de recopilar toda la información de su host, la cual es enviada hacia el servidor donde se realiza su filtrado y procesamiento, en algunos casos solo es libre la parte cliente, o sea, la que se instala en cada una de las computadoras de la red. Sin embargo la parte servidor si es privada, teniendo que pagar para poder hacer uso de ella.

Actualmente muchas empresas e instituciones gastan mucho dinero en la recolección de los logs generados en sus sistemas manualmente, lo que evidentemente provoca pérdida de tiempo, además de que es muy probable que no se detecten algunas infracciones o errores imposibles de ver a simple vista, no existirá una reacción en tiempo real contra estas anomalías y que muchas veces será tarde.

1.2.1.5 Criterios y requisitos utilizados en la recolección de registros de eventos.

Debido a que la información que se almacena en los logs puede ser utilizada como evidencia digital (por evidencia digital se entiende toda información obtenida a partir de una computadora o equipo electrónico que permite el esclarecimiento de algún hecho delictivo o ayuda a vincular al autor con el propio hecho), en la actualidad se les da mucha importancia, por lo que se han redefinido determinados criterios indispensables a tener en cuenta para ser usados en un posible caso judicial:

- **Autenticidad**: donde todo lo que se considere evidencia digital deberá cumplir con que se debe demostrar que toda la información ha sido generada en el lugar y momento en que ocurrieron los hechos. Además de que esta evidencia debe demostrar que no ha sido modificada ni ella ni los medios.
- **Confiabilidad**: para que los registros que han sido tomados como evidencias sean confiables, sus fuentes deben de ser creíbles y que se puedan verificar.
- **Respeto y apego a las leyes**: la evidencia digital debe cumplir con los códigos y normas establecidos en las leyes del país o región en que fue generada.
- **Completitud o suficiencia de la evidencia**: es necesario que la información que se utiliza como evidencia digital sea completa, que brinde toda la información posible y que no haya sido alterado su contenido.

El momento de recopilar la información que será utilizada como prueba de la ocurrencia de algún hecho es muy importante ya que si no se realiza de la forma adecuada o no se incumplen determinados parámetros puede que esa información no sea confiable por lo que no pueda ser utilizada ante las leyes como evidencia digital. Para el manejo de la información es necesario cumplir con determinados requisitos:

- Lo primero es que se debe recopilar la información a través de los procedimientos establecidos por la ley y la información que se obtenga debe de ser recopilada en medios de almacenaje

confiables, como pueden ser los de solo escritura (ejemplo CD), y de ser posible depositar este en un lugar seguro.

- El lugar donde sea guardada la evidencia debe tener la seguridad de que no pueda ser accedido por terceras personas como puede ser en una caja fuerte, pero que debe ser accesible para los autorizados y responsables de la investigación.
- Hay que verificar siempre que el personal encargado de recopilar la información esté conformado por personas que cuenten con la debida calificación para estas actividades.

Se debe hacer un constante seguimiento al proceso de recopilación de la información para verificar el cumplimiento de las normas establecidas, donde la institución o la persona encargada de llevar a cabo estas acciones deben velar por la integridad de los datos.

1.2.1.6 Protocolos más utilizados en el transporte de logs.

Para la recolección y procesamiento de eventos muchos sistemas hacen uso de algunos protocolos, a través de los cuales se logra una mayor seguridad y eficiencia en su trabajo. A continuación veremos algunos de ellos:

Syslog: El Syslog básicamente es un sistema de logs, también se le conoce como protocolo, aplicación o biblioteca, que fue pensado para la administración y control de los eventos generados tanto por el sistema operativo como por las demás aplicaciones y el kernel. En sus inicios fue usado para registrar los logs generados por el sistema y otras aplicaciones así como la red, en sistemas operativos basados en Unix. El protocolo Syslog está formado por un emisor que se encarga de enviar mensajes a través del protocolo UDP en texto plano a un receptor, que es el llamado Syslogd, que constituye el servidor. Este puede ser configurado para recibir eventos de otros dispositivos que soporten el Syslog como los firewalls, routers.

NTP: Por sus siglas en inglés “Network Time Protocol” o Protocolo de Tiempo de Internet. Se usa para sincronizar la hora de los clientes instalados en los PC y en los Servidores, tomando como referencia otro Servidor o fuente de tiempo (como puede ser un receptor de satélite). En los sistemas de recolección de logs pueden ser muy importantes ya que proporciona la coordinación necesaria entre el servidor y los clientes para el envío de los logs. Así existirá fiabilidad en cuanto a la fecha y hora de la ocurrencia de los eventos.

SNMP: El protocolo SNMP (Simple Network Management Protocol) o Protocolo Simple de Administración de Red se utiliza en la administración de redes donde se encarga de gestionar la configuración de los dispositivos conectados para el intercambio de información a través de esta. Forma parte de la familia de protocolos para internet y es no orientado a la conexión, contribuye en que lo que hace como parte de las tareas de la administración de la red no disminuirá el rendimiento de la misma, ya que no utiliza los servicios orientados a la conexión. SNMP utiliza generalmente los puertos 161 y 162.

TCP: Son las siglas de Protocolo de Control de Transmisión (por sus siglas en inglés Transmission Control Protocol), utilizado para la transmisión de datos por la red. Es orientado a la conexión, lo cual lo asemeja a la telefonía donde para poder hablar o transmitir datos en este caso primeramente se debe establecer la comunicación entre ambas partes.

UDP: Son las siglas de Protocolo de Datagrama de Usuario, (por sus siglas en inglés User Datagram Protocol), usado para la transmisión de datos a través de la red. Es un protocolo no orientado a la conexión, característica que lo asemeja al correo postal, donde no se necesita establecer comunicación entre el origen y el destino de los datos para enviarlos ya que estos contienen la suficiente información acerca de hacia donde son enviados encaminándose ellos mismos.

1.2.1.7 Herramientas desarrolladas para la recolección de logs.

Como parte del amplio trabajo que se ha desarrollado a nivel mundial sobre la recolección centralizada de los logs, se han desarrollado muchas herramientas con este fin. Muchos de los sistemas existentes se especializan en la recolección de tipos específicos de eventos, mientras otros son capaces de trabajar con varios formatos de logs. Algunos de dichos sistemas han sido utilizados en Cuba y en la UCI específicamente. Actualmente los grupos de desarrolladores de sistemas de recolección de eventos han implementado software en las tres formas posibles en que se puede desarrollar un sistema de este tipo: Agente, Servidor y Cliente-Servidor, algunos son libres y otros propietarios, de los cuales a continuación se describen los más importantes:

Agente o Cliente

Son sistemas que al ser instalados en una PC realizan la función de recoger los eventos ocurridos en la propia PC para su almacenamiento y posterior análisis. En este grupo existen sistemas que brindan la posibilidad de enviar la información hacia un servidor que sea compatible con este, aunque existen

otros que no cuentan con esta funcionalidad, por lo que solamente son usados para monitorear los logs ocurridos en una sola PC. Como ejemplos tenemos:

Logwatch

Debido al gran volumen de información que se pueden generar en los logs y a la gran gama de tipos que pueden existir, es necesario que sean leídos periódicamente. Todo esto depende también de la cantidad de acciones que se realicen en la computadora, aunque sería muy factible hacerlo diariamente. El Logwatch es una herramienta muy buena para casos de este tipo ya que se encarga de generar reportes de forma sencilla, que son enviados por correo electrónico, y que pueden ser leídos por el administrador. Para un sistema de uso personal su utilidad es bastante relativa, siendo mucho más útil en un servidor que es más susceptible de ser monitorizado.

Lasso

El grupo LogLogic, fundado en el año 2002 en San José, California, ha desarrollado la herramienta Lasso con el objetivo de recolectar los eventos de Windows. La empresa cuenta con muchos empleados y clientes en varias partes del mundo, entre ellos bancos, instituciones dedicadas a las ciencias biológicas, gas y petróleo, etc. Lasso cuenta con muchas ventajas entre ellas que es de código libre como todas las herramientas desarrolladas por el grupo LogLogic. Además que fue implementado para enviar los eventos recopilados hacia un servidor Syslog compatible como Syslog-ng.

Servidor

Los servidores son la parte más importante del sistema ya que son implementados para recibir información enviada por los agentes que sean compatibles con ellos acerca de la ocurrencia de eventos en las computadoras donde estos estén instalados. En estos servidores pueden ser capaces de realizar filtrados, auditorías, reportes, e incluso graficas y enviar alertas, todo en dependencia del nivel de implementación que se le haya realizado.

Servidor SPLUNK

La compañía Splunk fue fundada en 2003 y su primer producto salió en 2005 con el mismo nombre.

Splunk es una aplicación web muy popular para Linux que les da a los administradores de redes una amplia visión de los datos contenidos en los ficheros logs. Esta herramienta fue implementada para hacer la función de servidor de diferentes clientes en la recopilación de eventos. Sus desarrolladores lo

pensaron para que pudiera recibir y entender la información recogida por un gran número de agentes como los de SNARE y Syslog.

El Splunk constituye una de las herramientas más avanzadas en la gestión de los logs a nivel mundial la cual es capaz de indexar datos en cualquier formato enviados desde cualquier fuente en tiempo real, incluyendo logs, configuraciones, scripts, código, mensajes, alertas, reportes de actividades, desde todas las aplicaciones, servidores y dispositivos. Permite buscar, navegar, alertar y hacer reportes de toda la información en tiempo real a través de una interfaz web desarrollada en AJAX. El equipo desarrollador de Splunk cuenta con una comunidad donde se comparten conocimientos y soluciones a través de SplunkBase.com, el sitio donde se realiza intercambio de criterios sobre la herramienta. Fue desarrollado en los lenguajes de programación C, C++ y Python.

Cliente-Servidor

El sistema más completo es el que cuenta con clientes y servidor. Actualmente existen grupos desarrolladores que cuentan con su propio cliente y servidor. Como ejemplos existen los siguientes.

GFI EventsManager

GFI EventsManager es un sistema muy completo y que cuenta con muchas facilidades para los usuarios como se detallan a continuación:

- Recolecta todos los logs generados por todas las computadoras y servidores que existan conectados a la red, ya sean de aplicación, sistema, seguridad, sucesos de servidores DNS, etc. a través de su propio agente, además de que en tiempo real detecta posibles violaciones o ataques, alertando a los administradores.
- Es capaz de realizar una copia de respaldo de la información y a la vez eliminarla de todas las computadoras automáticamente.
- Muchos sistemas de este tipo realizan la recopilación de la información máquina a máquina, pero el GFI EventsManager tiene una ventaja y es que lo realiza en toda la red, haciendo informes y filtrando los eventos.
- Se vende conjuntamente con un Servidor Syslog integrado que se encarga de recoger automáticamente los logs enviados por los agentes Syslog.

- Cuenta con una base de datos centralizada en la cual se pueden hacer filtrados y análisis de toda la red de forma personalizada, a intervalos deseados y en tiempo real.
- Es capaz de enviar alertas en tiempo real vía e-mail a uno o más destinatarios.
- Es de tipo propietario.

Herramientas de Syslog

El sistema de registros Syslog cuenta con un gran número de versiones incluso para el sistema operativo Windows. Actualmente ya existe el Syslog-ng o Syslog-New Generation por sus siglas en inglés (Syslog-Nueva Generación) superior al Syslogd, el cual cuenta con algunas ventajas como la de que brinda la posibilidad de usar TCP para el envío de la información a través de la red además de que los datos viajan cifrados usando SSL/TLS. Este servidor es muy potente y puede recibir datos desde muchas fuentes que soporten el Syslog.

Para las distintas versiones del sistema operativo Windows también Syslog cuenta con su herramienta. El trabajo con los logs de Windows o EventLogs se dificulta mucho teniendo en cuenta que los ficheros de almacenamiento se guardan de forma binaria. NTSyslog fue desarrollado para recopilar los eventos de Windows y enviarlos hacia un servidor Syslog remoto.

Otra herramienta es el Klogd, el cual se encarga de la recepción de los mensajes enviados pero con la particularidad de que solo los enviados por el Kernel. Es importante destacar que el servidor únicamente recibe mensajes de otros servidores, computadoras, etc., que se encuentran en su misma red y equipo de trabajo.

Intersect Alliance

Intersect Alliance es un equipo con mucha experiencia en lo que a seguridad se refiere, siendo especialistas tanto en la teoría como en la práctica de las políticas de seguridad. Dentro del gran grupo de herramientas que desarrollan están sistemas tanto libres como propietarios. Su base principal radica en Canberra, Australia y cuentan con clientes en todo el mundo, tanto corporaciones y fundaciones económicas, financieras y de las telecomunicaciones como agencias gubernamentales. Son muy conocidos por ser el desarrollador del primer software de recolección y auditoria de eventos logs y de código abierto para el sistema operativo Linux.

Su grupo de herramientas conocidas como SNARE (por sus siglas en inglés System iNtrusion Analysis & Reporting Environment) o Entorno de Análisis y Reporte de Intrusión al Sistema, cuentan con un gran prestigio a nivel mundial. Debido a que su sistema está desarrollado bajo la arquitectura cliente-servidor, consta de dos aplicaciones: los agentes de SANARE (SNARE Agents) y demás Herramientas, el cual se instala en cada una de las computadoras o dispositivos de la red desde donde es el encargado de enviar hacia el servidor central los eventos ocurridos, y un servidor SANARE (SNARE Server) que se instala en el servidor central donde se realiza la mayor parte de la gestión y auditoria de la información recibida desde los distintos agentes. Es importante tener en cuenta que Intersect Alliance brinda el software que se instala en las computadoras como agente de forma libre, sin que haya que pagar para descargarlo ni utilizarlo, pero la parte servidor si es propietario teniendo que pagar por hacer uso de este. Incluso los agentes que son libres tienen algunas restricciones y no cuentan con algunas funcionalidades. Sin embargo para los clientes que compren el servidor tienen acceso a los agentes con todas sus herramientas.

Este grupo no solo ha desarrollado sistemas para Linux, sino que además para casi todos los sistemas operativos existentes y que son las más utilizadas, como: Solaris, Windows NT/2000/2003/XP, Netware, Tru64, Linux, AIX, IRIX y otros, de algunos de los cuales se da una descripción a continuación, así como de otras herramientas que conforman el grupo SNARE.

Agentes de SNARE (System iNtrusion Analysis & Reporting Environment) y demás Herramientas.

El conjunto de herramientas SNARE cuenta con un gran número de agentes para distintos sistemas operativos y servidores. Además de esto también han desarrollado agentes para muchos tipos de servidores y dispositivos. Es importante saber que para todos los agentes la capacidad de enviar usando el protocolo TCP y la posibilidad de enviar hacia múltiples servidores está solo disponible para aquellos que hayan comprado el servidor y tengan soporte para sus agentes. Veremos algunas de estas herramientas a continuación.

SNARE BackLog

SNARE BackLog es un programa que cuenta con una facilidad para el procesamiento central de eventos desde una variedad de fuentes de log, incluyendo Agentes de SNARE para Windows, Solaris, AIX, IRIX, el Servidor de ISA, el Servidor de IIS, Lotus Notes y otros, más cualquier dispositivo capaz de enviar los datos a un servidor en formato Syslog. Fue desarrollado para trabajar sobre Windows

solamente y utiliza el protocolo UDP por los puertos 6161 (que es el puerto que utilizan por defecto los agentes de SNARE) o 514 que es el nativo de Syslog. Los eventos deben ser enviados hacia el BackLog por Agentes de SNARE, cualquier versión de Syslog o aplicación que pueda enviar los datos a través de los puertos antes mencionados. Estos puertos se han definido de manera fija por lo que no pueden ser cambiados. Luego de recibir los eventos los almacena en un fichero, el cual puede ser definido y nombrado por el usuario.

Es llamado el hermano pequeño del 'Servidor SNARE' debido a que el servidor de SNARE proporciona una colección robusta, analizando, reportando y archivando el entorno, usando una interfaz web, y el almacenamiento en una base de datos. Sin embargo SNARE BackLog contiene sólo el componente básico de 'recolección', sin las capacidades de procesamiento de los datos. Además cuanta con una interfaz, que no es Web, muy sencilla a través de la cual se visualizan los 1000 eventos más recientes recibidos, además de algunas opciones de configuración de la herramienta.

SNARE Epilog para UNIX, SNARE Apache y SNARE Squid:

El agente de SNARE Epilog (o Epílogo del español) para UNIX opera a través del proceso "Epilog", así monitorea los logs y controla los eventos generados basados en los objetivos definidos en el fichero de configuración. Los ficheros de logs son filtrados usando los objetivos, etiquetados de acuerdo con el tipo de logs que son y enviados a través de la red usando el protocolo UDP ó TCP hacia uno ó más servidores para su posterior análisis y archivado. Todas las funciones del Epilog par Unix pueden ser controladas remotamente a través de un navegador web estándar.

El SNARE para Apache y el SNARE para Squid son módulos del Epilog que permite el registro de eventos del Apache y del Squid respectivamente.

Agente de SNARE para Linux:

El equipo de InterSect Alliance tiene la experiencia con auditoría y detección de intrusión en un gran número de plataformas como - Solaris, Windows 2000/NT/XP/2003, AIX, y otras; y dentro de la amplia gama de los IT (Tecnologías de la Información) en la seguridad de empresas como la Seguridad Nacional y Agencias de Defensa, empresas de Servicio Financieras, Departamentos Gubernamentales y Proveedores de Servicio. Actualmente el equipo de InterSect Alliance está trabajando también en el subsistema de auditoría existente para las posteriores generaciones del Kernel de Linux, para lograr desarrollar un subsistema que sea simple y eficaz para las distintas distribuciones de Linux. El

proyecto se llama “SNARE for Linux” o SNARE para Linux y como muchos otros Agentes de SNARE y demás herramientas está disponible bajo las condiciones de la Licencia Pública de GNU.

Agente de SNARE para Windows:

El agente de SNARE para Windows (para cualquiera de las versiones WINDOWS NT, Windows 2000, Windows XP, y Windows 2003) es un servicio compatible que actúa recíprocamente con el subsistema de auditoría nativo de Windows Eventlog para facilitar remotamente la transferencia en tiempo real de la información de los logs de eventos. Los logs de Seguridad, Aplicación y logs de Sistema, así como los nuevos DNS y los logs del Directorio Activo son recogidos por el agente de SNARE para Windows. El dato contenido en el log se convierte al formato de texto, y se envía hacia un Servidor de SNARE remoto, o a un servidor de Syslog para su procesamiento.

Agente de SNARE para Solaris:

El agente de SNARE para Solaris trabaja a través de las funciones del demonio o servicio “SNARECore”, el cual interactúa con el kernel del SO (Sistema Operativo) para leer, filtrar y enviar los logs de eventos desde el Subsistema de Registro de Eventos (conocido en Solaris como Basic Security Module ó BSM por sus siglas en inglés o Modulo Básico de Seguridad del español) hacia un servidor remoto. Los eventos que serán enviados dependerán de los objetivos definidos y no de la configuración del los ficheros del BSM, debido a que automáticamente el agente tomará el control del subsistema BSM sin la intervención de ningún administrador del sistema, los logs serán entonces filtrados de acuerdo con los objetivos escogidos por el propio administrador y enviados a través de la red usando los protocolos TCP ó UDP hacia un servidor remoto.

El SNARECore convierte los eventos logs de Solaris del formato binario a formato de texto y cuenta con una herramienta la cual se encarga de controlar los posibles fallos que ocurran donde luego de la ocurrencia de alguno reinicia el servicio. Además puede ser controlado remotamente usando un navegador web estándar.

SNARE Generator

El SNARE Generator fue diseñado para generar eventos artificialmente y enviarlos al servidor de SNARE a través de la red. Es capaz de generar 5 tipos de eventos: eventos de Windows, de Solaris, IRIX, SYSLOG y de PIX (CISCO firewall). Originalmente fue desarrollado para hacerle pruebas al servidor. Es capaz de realizar algunas de las funciones que realiza el servidor pero no las más

importantes y puede ser configurado de diferentes formas, la más sencilla es a través del menú de "Configuration" ó Configuración en su traducción al español.

Servidor SNARE

El servidor de SNARE permite a los administradores de redes definir, rastrear y reportar la ocurrencia de acciones malignas a partir de los eventos ocurridos en el servidor. A su interfaz se puede acceder a través de un navegador web estándar. Actúa como el sistema recopilador central, recibiendo un gran flujo de información desde los agentes y cuenta con un grupo de objetivos de seguridad que permiten hacer un filtrado de los eventos enviados desde los distintos agentes. El principal rasgo del servidor SNARE es la habilidad para definir objetivos complicados de seguridad en un fácil lenguaje de programación, para reportar los descubrimientos de una manera simple pero concisa, y proveer la información necesaria para la seguridad profesional. SNARE fue originalmente desarrollado para responsabilizarse por las necesidades de auditoría de organizaciones que requerían una seguridad significativa, la mayoría de las cuales son agencias de Comunicaciones Inteligentes y el Departamento de Defensa.

IDS y OSSEC

En el campo de la seguridad constituyen una herramienta muy eficaz los IDS ó Sistemas de Detección de Intrusos, los cuales como su nombre indica permiten detectar posibles acciones malignas al sistema o la red, así se podrá saber cómo y cuándo ocurrió el ataque e incluso efectuar acciones reactivas ante estos ataques.

Existen 3 tipos de IDS:

- IDS en Host (HIDS): los sensores o agentes se encuentran en cada máquina y por tanto vigilan únicamente dicha máquina.
- IDS en Red (NIDS): los sensores se encuentran en segmentos de red y por tanto vigilan el tráfico de la misma.
- IDS Distribuidos (DIDS): en la práctica se trata de una serie de NIDS que se comunican con un sensor central.

La característica fundamental de los HIDS es que su sistema está formado por dos partes principales:

- Los agentes: se instalan en cada una de las computadoras de la red, desde donde recopilan la información necesaria de las incidencias ocurridas en esta y luego la envían hacia el servidor para un procesamiento centralizado. También suelen ser llamados sensores.
- El servidor: este es el centro de toda la herramienta, recibiendo todos los datos provenientes de los distintos agentes instalados por toda la red. A partir de la información recibida es capaz de realizar reportes de incidencias ocurridas e incluso detectar posibles ataques o vulnerabilidades.

Muchos de los HIDS se basan en la recolección y análisis de los eventos ocurridos en las computadoras para detectar incidencias negativas. Dentro del grupo de HIDS y que realiza la recolección de eventos se encuentra el OSSEC, el más potente y reconocido de los de su tipo. OSSEC proporciona recolección y análisis de logs, verificación de integridad de ficheros, y otras funciones. Para ello fue desarrollado conjuntamente con el servidor los respectivos agentes para los sistemas operativos Windows, para muchas de las versiones de Linux y otras. El servidor hasta el momento solamente está desarrollado para trabajar sobre Linux. Un problema presente en los sistemas de IDS es que aunque proporcionan muchos beneficios, la gestión de las alertas resulta ser muy tediosa, para ello OSSEC cuenta con una interfaz web escrita en PHP que permite la consultar y visualizar rápida y sencillamente las alertas.

Applications Agent

El equipo Barcelona/04 Computing Group, fundada en 1991 en Barcelona creó el sistema Applications Agent, como parte del conjunto de herramientas Barcelona/04 VISUAL Message Center, las cuales realizan acciones de monitoreo, gestión de la seguridad, alerta, informes, automatización, entre otros.

Entre las cosas que distinguen al Applications Agent está la posibilidad que tiene de leer una gran cantidad de líneas de cualquier tipo de logs en texto plano y cualquier formato, incluso los definidos por el usuario o formato libre, en poco tiempo, y cuenta con una consola para mostrar los resultados gráficamente. Otra de las ventajas es que es capaz de hacer la lectura de los reportes generados en los logs en tiempo real, o sea, cada vez que se genera una nueva información en los logs los lee, por lo que no es necesario tener que hacer una lectura periódica de todos los registros, lo que indudablemente reportaría un mayor gasto de tiempo además de que sobrecarga la red.

Incluye conectores predefinidos para monitorizar logs de aplicaciones como Apache Web Server, Microsoft ISA Server y SQL Server. Así, Applications Agent monitoriza virtualmente todas las aplicaciones existentes hoy en día y está preparado para gestionar las que todavía están por venir. Applications Agent al igual que las demás herramientas desarrolladas por la empresa Barcelona/04 Computing Group es de tipo propietario. (Barcelona/04 Computing Group, 2004)

Samhain

La herramienta Samhain fue desarrollada para entre otras funcionalidades recopilar los eventos ocurridos en las computadoras que trabajaran con el sistema operativo Linux. Para ello cuenta con su propio cliente y servidor. Actualmente se ha desarrollado una aplicación en PHP y C llamada Beltane que permite visualizar los eventos recopilados per el servidor de Samhain.

Para los sistemas operativos Linux existen comandos que permiten ver y procesar los logs de una PC, además por defecto todos los logs se almacenan generalmente en la dirección **/var/log**, algunas versiones lo hacen en **/var/admin,** aunque se pueden almacenar donde desee el usuario. Para las personas que tienen una computadora en su casa o en su oficina de trabajo, y que no forme parte de una red con un sistema de recolección de eventos centralizado estos comandos pudieran ser muy útiles si se desea saber las incidencias ocurridas en la máquina. A continuación se describen algunos de ellos:

- **Cut:** se encarga de dividir una línea de texto en campos, permitiendo la selección de uno o varios de ellos.
- **Host:** permite conocer el nombre de un host y dominio a partir de un IP.
- **Sort:** este comando ordena alfabéticamente todos los resultados.
- **Grep:** para filtrar líneas de ficheros a partir de expresiones regulares.

Para los sistemas operativos Windows este permite ver todos los eventos ocurridos en el sistema a través de un Visor de Sucesos, al cual se puede acceder a través de clic derecho en Mi PC, seleccionar Administrar, y en la parte superior izquierda aparece la opción antes mencionada. La ventana mostrará los EventLogs de Windows clasificados en Sistema, Seguridad y Aplicación.

1.2.2 En Cuba.

A partir de investigaciones hechas se ha comprobado que en Cuba la experiencia que existe en los sistemas de recolección de logs es muy poca. En gran medida esto se debe a que no ha existido un gran desarrollo en la informática y las telecomunicaciones. Pero con los avances que se han venido obteniendo en estos campos en todo el país y a partir de la necesidad de lograr una mayor seguridad y desarrollo en sus instituciones, la informática cubana siente la necesidad de ponerse a la par del resto del mundo, todo esto dentro de los programas que lleva a cabo la Revolución cubana. La UCI, como uno de los principales programas de la Batalla de Ideas no se queda atrás, pero no es la única institución donde se han desarrollados trabajos sobre el tema de la gestión de la seguridad de la red y más específicamente de la recolección de logs. Como muestra de ello está SALDI o Sistema Analizador de Logs para la Detección de Intrusos desarrollado en la CUJAE (Ciudad Universitaria José Antonio Echeverría), la idea desarrollada por la fundación EHAS (Enlace Hispano Americano de Salud) y la estrategia del portal www.cuba.cu a través del Webalizer, las cuales se detallan a continuación.

SALDI

Con el objetivo de aumentar la seguridad de la red de computadoras de la CUJAE y aliviar las tareas de los administradores por medio de la administración centralizada de un sistema IDS y el análisis de los Logs generados por servicios instalados en servidores Linux, así como ayudar al trabajo reactivo a corto plazo del administrador se desarrolló la idea de implementar el SALDI. Este sistema es capaz de realizar análisis de eventos con diferentes intervalos de tiempo, crear y enviar reportes por correo, almacenar los reportes en una Base de Datos, y otras funciones. Para su desarrollo se utilizaron como lenguaje de programación Perl, PgAdmin como aplicación gráfica para el manejo de la Base de Datos en PostgreSQL y Macromedia Dreamweaver para desarrollar la página web.

Idea desarrollada por la Fundación EHAS

La Fundación EHAS es una institución sin ánimo de lucro, fundada en la Universidad Politécnica de Madrid (UPM) cuyo único fin es la mejora de los sistemas públicos de asistencia de salud en las zonas rurales de los países hispanoamericanos, y todos aquellos otros que se encuentren en vías de desarrollo, a través del uso de las nuevas tecnologías de la información y las comunicaciones.

Hasta la fecha de hoy, EHAS ya tiene instaladas varias redes en Perú, Colombia y Cuba con cierto nivel de complejidad, con puntos conectados a Internet de forma permanente y muchos otros con conexiones intermitentes por radio. Actualmente EHAS no tiene implementado en sus instalaciones

ningún mecanismo para facilitar la monitorización centralizada de las redes. El estado de la red es globalmente desconocido, no se sabe inmediatamente cuándo se produce un evento que requiera intervención y desde luego no se tiene información sobre el deterioro de los sistemas para prevenir algunas averías antes de que se produzcan.

Para esta problemática se trazaron un conjunto de acciones a realizar:

- **SNMP**: El protocolo SNMP es el estándar más extendido para la gestión centralizada de redes. Su uso en los sistemas de EHAS pasa por el soporte y activación en los sistemas que se quieran monitorizar, y en desarrollo o adopción de herramientas que recojan esa información y le den el tratamiento necesario para presentarla de forma sintética y fácilmente comprensible, normalmente mediante gráficas y tablas.
- **Envío de logs por e-mail**: En la UPM se desarrolló un sistema de recolección de logs lo más sencillo y extensible posible. Se trata de que los puestos cuya única forma de comunicación es el correo electrónico puedan reportar información sobre su estado por este medio, o sea, a través del correo. Para lograr la sencillez y extensibilidad deseada, el sistema permite definir con expresiones regulares las cadenas que son importantes y pasar un grep con ellas al Syslog. La información se envía de forma diaria desde los servidores y semanal desde los clientes. En la configuración de cada estación se configura la periodicidad con que se quiere que se registre en los logs cada información.

  De partida hay 4 tipos de logs que se reportaron: correo electrónico, placa, radio y modem telefónico. También se recogen los encendidos y apagados ordenados del ordenador. La información se recoge en un servidor, que la procesa con Procmail y la pone en una base de datos Postgres.
- **Plan de trabajo provisional**: Por el momento se trabaja en la ampliación de estas acciones hasta que incluya todos los aspectos y detalles que sean pertinentes para trabajar en una solución de gestión de redes EHAS con el mejor enfoque posible. Los actores involucrados deben enviar a la dirección técnica toda sugerencia o aportación que pueda tenerse en cuenta para poner en práctica en la gestión de la red. (EHAS, 2004)

Uso de Webalizer en el portal www.cuba.cu.

El portal cubano www.cuba.cu desarrolló un estudio para tratar de conocer cómo los usuarios utilizan sus contenidos y servicios, una vez conocido estos, realizar un plan de medidas a corto, mediano y largo plazo para perfeccionarlo, que no sólo abarcara el diseño de interfaz e información sino también orientado a los servicios que se brindan en el sitio. Para ello se utilizó la herramienta Webalizer.

La herramienta Webalizer analiza la bitácora, como también se le llama a los logs, del servidor web y realiza reportes de los datos que contiene en forma de gráficas. Aquí se pueden ver los sitios y archivos más accedidos desde la página, los buscadores más utilizados para acceder a dicho sitio, etc. La información obtenida puede ser vista por el administrador del sitio en el navegador. Para dicho estudio se analizaron los logs generados por el portal entre Septiembre de 2002 hasta Agosto de 2003 y fue posible determinar la forma en que los usuarios utilizan el portal así como los temas que buscan y prefieren, y aquellos que no son relevantes para los mismos. (Coutin, et al., 2003)

1.2.3 En la UCI.

En la universidad de las Ciencias Informáticas se ha trabajado muy poco sobre el trabajo con los logs en general. Durante un tiempo se trabajó con la herramienta Event Log Security Manager, la cual es de tipo propietaria por lo que se debió descontinuar su uso. El funcionamiento de esta estaba basado en que en cada docente se instaló un servidor para que recogiera los eventos de las computadoras pertenecientes a esa área solamente. Luego se trabajo en la instalación y configuración de un servidor central que recibiera de todos los servidores instalados en los docentes de la universidad, donde se definieron reglas para el filtrado de los eventos recibidos. Como política de seguridad se adoptó que los sistemas operativos generaran determinados logs que pudieran ser importantes para la gestión de la seguridad. Durante el año 2007 el compañero Robmay García Fuentes especialista general de la Dirección de Laboratorios desarrollo una investigación acerca de las distintas herramientas de Syslog, logrando realizar algunas configuraciones poco profundas.

1.3 Conclusiones

En este capítulo pudieron observar el nivel en que se encuentra el trabajo con la recolección centralizada de los logs tanto en la UCI, en Cuba como en el resto del mundo. En la Universidad de las Ciencias Informáticas no se ha trabajado mucho y no se realiza la centralización de logs, de ahí surge la necesidad de encontrar un sistema capaz de recopilar los logs de las computadoras en las Áreas de

Riesgo. En Cuba, se vio como el trabajo ha sido poco también aunque a nivel mundial si existe una experiencia muy amplia, se han desarrollado un gran número de sistemas con características muy particulares, siendo algunos libres sin tener que pagar para usarlos mientras otros son comerciales teniendo que comprar una licencia para poder emplearlos. Dentro de este gran grupo de herramientas existen algunas que cuentan con muchas potencialidades para ser aplicadas en la UCI.

CAPÍTULO 2: SELECCIÓN DE LAS HERRAMIENTAS A UTILIZAR.

2.1 Introducción

En la actualidad son muchos los sistemas y dispositivos que generan eventos y todos pueden ser objetivos de algún ataque. Debido a esto es que se han desarrollado herramientas capaces de recopilar los eventos que ocurren en las computadoras, incluso algunos se han especializado en determinados tipos de eventos. En la Universidad de las Ciencias Informáticas se cuenta con una red muy grande, contando dentro de ellas con servidores y un gran número de laboratorios y aulas de las que se hace necesario almacenar toda la información que ocurre en sus computadoras. En este capítulo se tratarán las posibles soluciones existentes pero que debido a las condiciones de la red se hace imposible optar por algunas de ellas, hasta que se definirá la solución más óptima para la problemática planteada en el capítulo anterior.

Actualmente los sistemas que se ha desarrollado para la recolección de logs trabajan sobre la arquitectura cliente-servidor. En cada computadora o servidor de donde se necesite recolectar sus eventos se instala un agente que realiza el trabajo de recoger estos eventos y enviarlos hacia un servidor mediante alguno de los protocolos para el envío de datos a través de la red (más adelante se describirán los protocolos más usados para estas acciones). Existen sistemas completos, o sea, que cuentan con sus respectivos clientes y con un servidor que recibe lo que estos le envían. Existen otros donde sus desarrolladores solamente les han implementado uno de sus componentes, el cliente o el servidor, existiendo así la posibilidad de que se puedan integrar clientes y servidores de diferentes productos.

2.2 Rasgos a tener en cuenta para seleccionar un sistema para la recolección de logs en la UCI.

Durante el desarrollo del trabajo se tuvo en cuenta que dada las características de la red de la UCI y de la situación problémica planteada, existen algunos tipos de eventos que deben ser recolectados sistemáticamente para cuestiones de la seguridad y no todos los que se generan ya que algunos no brindan información de importancia. En las computadoras que estén trabajando sobre Windows se recogerán los de Seguridad. Para las computadoras que estén funcionando sobre las distribuciones de Linux se recopilará todos y entre los más importantes están los de Autenticación, los relacionados con los servicios de ejecución de programas, Mensajes del Kernel, Mensajes del propio Syslog, Mensajes

de los usuarios, etc. Además se recogerán los eventos generados por el Controlador de Dominio y el servidor de Squid.

De acuerdo con la situación problémica y las necesidades de la UCI se definió un conjunto de características que se debieron tener en cuenta a la hora de seleccionar un sistema para la recolección de los eventos, el cual está formado por agentes y un servidor central. Fueron las siguientes:

- La característica fundamental que se tuvo en cuenta fue que fuera libre en el sentido de tener acceso al código fuente y sin precio alguno. Más adelante se da una descripción detallada sobre el rasgo de ser “libre”.
- Debe ser multiplataforma, o sea que cuente con agentes para los distintos sistemas operativos instalados en las computadoras. En la UCI existen PC que trabajan con Windows y otras que lo hacen con alguna de las distribuciones de Linux como Ubuntu y Debian principalmente, por lo que se necesita que el sistema tenga soporte para estas plataformas.
- El servidor debe trabajar sobre alguna de las versiones de Linux. Como parte de una estrategia nacional de emigrar hacia software libre la UCI lleva adelante esta tarea, donde en un futuro todas las computadoras en el país trabajarán totalmente con sistemas de software que sean libres.

Para darle solución al problema presentado, un requisito fundamental como se planteó anteriormente y que se tuvo en cuenta fue que todas las herramientas que se utilizaran deberían ser libres. Actualmente viene surgiendo un movimiento a nivel mundial que opta por el desarrollo de software de manera libre haciéndole frente a los grandes monopolios de la informática y las comunicaciones como Microsoft. A continuación se presenta una de las definiciones que se le da al “software libre”:

El ``Software Libre" es un asunto de libertad, no de precio. Para entender el concepto, debes pensar en “libre” como en “libertad de expresión”, no como en “cerveza gratis” [en inglés una misma palabra (free) significa tanto libre como gratis, lo que ha dado lugar a cierta confusión].

“Software Libre" se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Un programa es software libre si los usuarios tienen todas estas libertades:

- *La libertad de usar el programa, con cualquier propósito.*

- *La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades. El acceso al código fuente es una condición previa para esto.*
- *La libertad de distribuir copias.*

La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. El acceso al código fuente es un requisito previo para esto. (Equipo de GNU, 2008)

2.2.1 Características de los protocolos TCP y UDP.

Un rasgo muy importante a la hora de implementar un sistema que transmitirá información a través de la red es el protocolo que utilizará para llevar a cabo esta tarea, aunque existen algunos que pueden hacerlo a través de varios de ellos. Entre las características que los diferencian está la velocidad con que se transmiten los datos, si son seguros o no, etc. El protocolo usado por un sistema debe influir a la hora de determinar si es el idóneo o no, de acuerdo con las características de la red donde será usado y los intereses de la institución. En la actualidad los más famosos son TCP y UDP, muy usados por parte de la mayoría de los sistemas de recolección de logs. A continuación veremos sus ventajas y desventajas en la transmisión de los datos.

UDP son las siglas de Protocolo de Datagrama de Usuario, (por sus siglas en inglés User Datagram Protocol), es un protocolo no orientado a la conexión (la conexión se realiza sin necesidad de que las partes se pongan en contacto anteriormente. Los datos enviados llevan suficiente información del destino como para llegar a este. Es análogo al correo postal donde el origen no establece comunicación con el destino, el propio mensaje contiene la información para llegar a su objetivo) y proporciona pocos servicios de recuperación de errores, en su lugar brinda una manera directa de enviar y recibir datagramas a través de la red. Se utiliza sobre todo cuando se necesita que la información llegue velozmente proporcionando un mejor uso del ancho de banda, aunque es menos seguro.

TCP son las siglas de Protocolo de Control de Transmisión (por sus siglas en inglés Transmission Control Protocol), es orientado a la conexión (deber existir un acuerdo entre las partes antes de realizar la conexión. Se hace una “llamada”, se hace una conexión y luego se establece la comunicación. Es análogo a la telefonía donde se hace la llamada y se mantiene la conexión.), garantiza que los datos enviados serán entregados a sus respectivos destinatarios sin errores, sin

pérdida, y en el mismo orden en que fueron transmitidos. Cuenta con un mecanismo para distinguir las distintas aplicaciones dentro de una misma máquina.

De estas características se resume que en aquellas instituciones donde la necesidad mayor es que los datos viajen por la red con mayor velocidad el protocolo más indicado es el UDP y en caso donde la prioridad es que la información sea transmitida con mayor seguridad se debe escoger el TCP.

2.3 Sistemas con potencialidades para ser utilizados en la UCI.

Existe un grupo muy grande de herramientas a nivel mundial que realizan las acciones de recopilación de eventos. Entre ellas evidentemente existen ventajas y desventajas. Durante la investigación el rasgo principal que se tuvo en cuenta fue de que los sistemas analizados fueran de código abierto y libres de pago monetario.

2.3.1 SNARE.

Intersect Alliance ha desarrollado los agentes de SNARE como código abierto y gratuito con el objetivo de ayudar a la comunidad en el campo de la recolección y monitoreo de logs, además de incrementar la fiabilidad y estabilidad de sus agentes. Dichos agentes son muy potentes, de fácil configuración e interfaz muy amigable.

El Agente de SNARE para Windows utiliza los protocolos TCP y UDP para el envío de información hacia el servidor por el puerto 6161. Es importante conocer que actualmente existen restricciones impuestas por parte del grupo de Intersect Alliance ya que la capacidad de enviar datos a través del protocolo TCP y la habilidad de enviar eventos a múltiples destinos solo está disponible para los usuarios que hayan comprado el servidor, con sus agentes correspondientes. Una opción muy importante es la de SNARE Filtering Objectives Configuration o Configuración de los Objetivos de Filtrado de SNARE a través de los cuales se tiene un gran control acerca de cuáles eventos son seleccionados y reportados. Ver Anexos Figura 10.

Ventajas de los agentes de SNARE:

- **Latencia y sus características en tiempo real**: los agentes de SNARE operan en tiempo real. Esto significa que cuando se genera un evento inmediatamente el agente se encarga de copiarlo y enviarlo al servidor. Por consiguiente esto significa que no haya latencia entre la generación del log y su recepción en el servidor, excepto por problemas del sistema operativo de la computadora o de la red entre esta y el servidor.

- **Control Remoto**: los agentes de SNARE pueden ser controlados completamente vía remota a través de un navegador. Esto significa que todos los aspectos de su operación pueden ser cambiados sin tener a un administrador haciendo los cambios. Desde que los agentes pueden cambiar la configuración nativa de auditoria del sistema operativo, si es que así lo decide el administrador, el usuario solo necesita cambiar el agente remoto para que los cambios surtan efecto.
- **Filtrado**: la mayoría de los sistemas operativos generan un gran número de eventos en cualquier circunstancia. Por esta razón es importante que los agentes sean capaces de filtrar estos eventos lo que contribuye con los requerimientos de seguridad de la organización. En algunas situaciones la mayoría de los eventos son necesarios, esto podría sobrecargar el servidor. Los agentes de SNARE incluyen la habilidad de filtrar eventos utilizando expresiones regulares o estándar por el contenido, tipo de evento, usuario o éxito/fracaso de un evento de grabado.
- **Control de auditoria del Sistema Operativo nativo**: la generación de eventos o los sub-sistemas de auditoria en los sistemas más modernos incluyen la funcionalidad de controlar cómo los logs de eventos son generados, configurados y producidos. En algunos sistemas esto puede ser muy complicado y confuso. Los agentes de SNARE son capaces de configurar el sub-sistema nativo si se desea y permitir que solo determinados eventos sean generados, lo cual es definido por las políticas de seguridad.

Otros beneficios del sistema SNARE

- El soporte de múltiples plataformas con agentes para las distribuciones más usadas como Windows y las distintas versiones de UNIX, así como para algunos dispositivos como firewall.
- La detección de actividad sensitiva (incluyendo el uso de cuenta especial con privilegios y acceso sensitivo para los archivos y los directorios).
- Fácil para usar la información y las capacidades de archivado.
- La congestión de la red reducida a través del uso de los agentes de SNARE.

2.3.2 Servidor Splunk.

La herramienta Splunk fue desarrollada por la compañía del mismo nombre fundada en el 2003 y su primera versión salió en el 2005. Fue implementado para realizar la función de servidor llegando a ser

reconocido como uno de los más potentes para la recolección y procesamiento de eventos, capaz de recibir datos desde múltiples fuentes como pueden ser los agentes de SNARE. Es capaz de indexar datos en cualquier formato enviados desde cualquier fuente en tiempo real, incluyendo logs, configuraciones, scripts, código, mensajes, alertas, entre otros. Cuenta con una interfaz web con muy buen diseño a la cual se puede acceder a través de cualquier navegador estándar. Ver Anexos Figura 15.

La principal ventaja del Servidor Splunk es que aunque no sea de código abierto o libre brinda una versión con una licencia libre, o sea que puede ser usado perfectamente sin tener que pagar por hacerlo. Además de esta versión se puede adquirir desde su sitio la versión privativa a través del pago de una cuota monetaria. La versión pagada cuenta además de las que tiene la versión libre con algunas funcionalidades que no están presentes en esta última, haciendo de este servidor una herramienta más potente, con mayor capacidad de recogida de datos así como que brinda otras opciones para el procesamiento de los eventos.

La versión libre presenta algunas restricciones que hay que tener en cuenta a la hora de escogerlo como receptor de eventos en una red tan grande como la de la UCI. Su principal inconveniente es en cuanto a la capacidad de procesamiento de eventos recibidos desde los agentes en un día, que actualmente es de 500 MB. Para redes pequeñas donde el volumen de información que se genera en los registros de eventos de sus computadoras y demás dispositivos es menor que esa capacidad, constituye un servidor muy idóneo. Dada las características de la red de la UCI, donde debido al gran número de PC que existen se genera una cantidad de información por los eventos mayor que 500 MB, este servidor no resultaría el más eficiente.

En las versiones de tipo propietarias el precio para adquirirlas varía de acuerdo con el volumen de información que pueden procesar. Los volúmenes de información que pueden recibir se encuentran entre más de 500 MB hasta sobrepasar los 10 GB. En correspondencia con esto los precios de adquisición también varían entre los 5000.00 $ y los 30 000.00 $.

2.3.3 OSSEC.

Su principal ventaja es que es libre. El creador y principal y desarrollador fue Daniel Cid, cuenta con una gran experiencia en el campo de los IDS, y con especial interés en la recolección y análisis de logs. El sistema OSSEC está formado por un servidor encargado de recibir toda la información enviada

desde sus propios agentes, además de que cuenta con una interfaz web muy sencilla y amigable. Ver Anexos Figura 16.

La conexión entre ambas partes es encriptada y se hace a través del protocolo UDP por el puerto 1514. Una peculiaridad de este sistema es la forma en que los agentes y el servidor se autentican, para ello se lleva a cabo un proceso donde en el lado del servidor se adiciona un agente a través de su dirección IP y se le asigna a un identificador o ID, luego de adicionarlo se genera una clave encriptada que debe ser exportada y copiada en el agente. De esta manera al conectarse el agente con el servidor se registra utilizando dicha clave, donde va contenido el ID que se le asignó en el servidor. El grupo desarrollador de OSSEC implementó este método para elevar la seguridad y fidelidad en los datos recibidos, por lo que solo los agentes registrados en el servidor podrán enviar datos hacia él.

Este servidor de OSSEC trabaja sobre cualquiera de las distribuciones de Linux y cuenta con agentes para las versiones de Windows y UNIX. Además de la posibilidad de recolección de eventos, OSSEC realiza otras actividades. A partir de los datos recibidos puede generar alertas de la ocurrencia de algún hecho negativo, tiene un sistema de detección de rootkit, realiza el chequeo sistemático de fichero, así cada ves que algún directorio ha sido modificado este lo registra. El servidor de OSSEC brinda la posibilidad de que todas las alertas que el servidor lanza puedan ser enviadas a través de un e-mail al administrador.

OSSEC soporta numerosos formatos de logs, entre ellos los generados por los distintos sistemas UNIX, servidores FTP, correos, y web, aplicaciones web, firewalls, base de datos PostgreSQL y MySQL, Squid, Windows y de algunos IDS como Snort. Para ello cuenta con una base de datos que puede ser en MySQL o PostgreSQL, la cual se crea a partir de un script que brinda el mismo equipo desarrollador y que se puede descargar del sitio de la herramienta.

2.3.4 Syslog.

El sistema operativo y otros subsistemas dentro de este constantemente generan un gran número de mensajes. Por ejemplo, los servidores FTP puede reportar cada conexión que se efectúe hacia él, el Kernel puede que reporte los fallos que ocurran en el hardware y los servidores DNS también puede reportar estadísticas en intervalos de tiempos. Indudablemente la información que puede generarse en una computadora debido a las acciones del usuario o a las del propio sistema es voluminosa. Algunos de estos mensajes necesitan ser analizados inmediatamente por parte de los administradores, otros puede que solamente necesiten ser almacenados para futuras referencias en caso de que exista algún

problema, y es posible también que se necesite extraer información de algunos de estos mensajes para realizar reportes.

Debido a esta situación la mayoría de los sistemas UNIX poseen la facilidad o herramienta “Syslog”, la cual guarda, analiza y procesa todos los archivos de registro sin requerir apenas intervención por parte del administrador. Actualmente Syslog cuenta con un gran número de variantes, algunas especializadas en tratar con tipos específicos de mensajes. Generalmente se basa en un demonio llamado “Syslogd”, el cual está a la escucha de los mensajes lanzados por el sistema.

Basándose en la clasificación de la información contenida en el mensaje y en la configuración del Syslog (esta configuración se encuentra usualmente en el fichero de la siguiente dirección **/etc/syslog.conf** pudiéndose transformar de acuerdo con los intereses del administrador), Syslog envía los mensajes en varios sentidos, por ejemplo:

- Enviarlos por e-mail a un usuario determinado.
- Escribirlo en un fichero de logs.
- Pasarlo hacia otro demonio.
- Descartar.

El demonio de Syslog puede también manejar mensajes de otros sistemas (cuando se dice “otros sistemas”, en este caso se trata de otras computadoras o dispositivos), para ello puede recibirlos a través del puerto de UDP. Para manejar los mensajes del kernel se utiliza otro demonio llamado “Klogd”, cuya especialidad es la de extraer estos mensajes para luego enviarlos hacia el Syslog como cualquier otro mensaje, pero propiamente identificado como que proviene del kernel. Los dos rasgos más importantes de los mensajes que maneja el Syslog son:

- Facilidad: se refiere a quién envió el mensaje. Existe un pequeño número de facilidades definidas, por ejemplo el kernel, el subsistema de correo y el servidor FTP.
- Prioridad: este valor indica qué tan importante es el mensaje. Corresponde a los números desde 0 hasta 7 en ese orden respectivamente. Los valores definidos para la prioridad son

    1. Emergency (Emergencia)
    2. Alert (Alerta)
    3. Critical (Crítico)

4. Error (Error)
5. Warning (Advertencia)
6. Notification (Notificación)
7. Informational (Informacional)
8. Debug (Depurar).

Syslog puede gestionar mensajes de múltiples fuentes como las siguientes:

- auth: Mensajes de autenticación.
- auth-priv: Mensajes de autenticación que no son creados por el sistema.
- cron: Mensajes relacionados con el servicio Cron.
- daemon: Mensajes relacionados con los servicios en ejecución.
- kern: Mensajes relacionados por el kernel
- lpr: Mensajes del servicio impresión.
- mail: Mensajes del servicio Mail.
- security (auth): Mismo eventos que auth.
- syslog: Mensajes del propio syslog.
- user: Mensajes de los usuarios.
- local0 a local7: Eventos personalizables por el usuario.

El Syslog tiene una dificultad y es que carece de interfaz, su funcionamiento es a partir de su archivo de configuración al igual que muchos de los sistemas que funcionan en UNIX. El trabajo con dicho archivo resulta ser un poco tedioso.

El Syslogd se desarrolló hace ya algunos años y aunque sea un poco antiguo su funcionamiento es muy bueno y no consume casi recursos. Sin embargo tiene debilidades en lo que a seguridad se trata. No realiza la transmisión de datos por la red a través del protocolo TCP, falta de información acerca del origen del evento y no realiza la encriptación de de los mensajes. Debido a esto han surgido proyectos con el objetivo de mejorar esta herramienta, un ejemplo de ello es Syslog-ng.

La versión más actual de Syslog es la Syslog-ng o Syslog-New Generation (Syslog-Nueva Generación). Debido a que el grupo desarrollador lanzó el producto bajo los términos de la licencia GPL hace que muchas de las distribuciones de Linux hayan adoptado al Syslog-ng como parte de su paquetería y actualizaciones. También existen versiones que son comerciales debiéndose pagar para poder adquirirlas, como el Syslog-ng Premium Edition, que constituye el agente de Syslog para los sistemas operativos Windows.

Por defecto al ser instalado no está configurado para enviar los mensajes hacia ningún destino, pero puede trabajar de tres formas diferentes dependiendo las necesidades de la institución. La forma en que deba trabajar se le configura en el archivo de configuración:

- Modo cliente: hace la función de agente recolector de eventos. Se instala en cada una de las computadoras que se desean monitorear enviando hacia el servidor las incidencias ocurridas en el host.
- Modo Relay: realiza la función de regulador entre los agentes y el servidor. Su trabajo consiste en recibir los mensajes enviados por los agentes y luego mandarlos hacia el servidor a través de la red, incluso puede mandar los propios eventos ocurridos en la PC donde esté instalado.
- Modo servidor: trabaja como recolector central de logs. Recibe mensajes desde los agentes y los Relay a través de la red y los almacena en su host o los reenvía hacia otras aplicaciones.

Cuenta con muchas ventajas con respecto a las demás que mejoran la infraestructura de registro de eventos:

- Ha incorporado el protocolo TCP para la transmisión de los datos a través de la red, el cual brinda más seguridad que el UDP tradicionalmente utilizado por Syslog.
- Realiza la encriptación de los datos.
- Se ha desarrollado una interfaz web, PHP-Syslog-ng, que aunque no viene dentro del paquete de instalación fue ideada propiamente pare visualizar desde la base datos a través de consultas y reportes la información almacenada de los eventos recibidos por Syslog-ng. Se puede acceder a ella a través de un navegador web. Una ventaja de esta interfaz en el sistema de autenticación lo cual le da más seguridad. Ver Anexos Figura 17.
- Puede trabajar sobre redes de tipo IPv4 e IPv6, recibiendo y enviando hacia ambos entornos.

- Tiene más criterios a la hora de realizar filtrados de los eventos almacenados en la base de datos.

2.3.5 Lasso.

La herramienta Lasso cuenta con muchas ventajas. Constituye un agente muy potente para recopilar todos los eventos ocurridos en el sistema operativo Windows y puede enviarlos hacia un servidor Syslog-ng a través del protocolo TCP, lo cual le da mayor seguridad en la transmisión de los datos. Aunque carece de interfaz realmente es tan fácil su configuración en su archivo de configuración que apenas se nota su ausencia. Luego de su instalación es necesario acceder a la carpeta de Lasso. Por defecto esta se guarda en C:\Archivos de programa\Lasso, donde está almacenada la configuración, diciéndole al agente el IP del servidor y el puerto entre otros valores. En la configuración se le pueden definir dentro de los grupos de logs de Windows cual o cuales serán enviados, por ejemplo Seguridad, Aplicación o Sistema.

2.3.6 SNARE Epilog para Squid.

El grupo Intersect Alliance ha desarrollado un agente para los sistemas UNIX, el Epilog para UNIX. Uno de los módulos que se pueden incluir en este agente es el SnareSquid, que permite la recolección de los logs del servidor Squid. Este módulo puede ser controlado a través de un navegador web. El Epilog para UNIX cuenta con un script que permite su fácil instalación, luego de la cual se puede adicionar el módulo SnareSquid para el trabajo en conjunto con el Epilog. Entre las opciones con que cuenta el Epilog está **Switch Configuration Files** que permite escoger con cual configuración se desea trabajar, o bien la de Epilog o la de Squid. Ver Anexos Figura 11.

2.4 Posibles soluciones.

Dentro del movimiento del software libre existe un tema muy importante y es la compatibilidad de aplicaciones, donde se puede observar en que medida sistemas que hayan sido desarrollados por diferentes instituciones o personas puedan trabajar en conjunto, aceptando mensajes, peticiones u órdenes unas de otros. Dentro de las herramientas para la recolección de logs también se puede observar este rasgo donde algunos servidores son implementados para que acepten los mensajes enviados por agentes que no son desarrollados por las mismas personas y así mismo, muchos agentes brindan la posibilidad de enviar hacia servidores de otros desarrolladores. Como ejemplo de lo antes expuesto está Splunk el cual dentro de los mensajes que puede recibir están los enviados por

los agentes de SNARE, los cuales a su vez también son capaces de enviar los eventos hacia un servidor Syslog. Por lo antes expuesto se presentan a continuación posibles combinaciones entre servidores y agentes que pudieran dar solución al problema planteado, teniendo en cuenta que para el servidor Squid el agente utilizado fue SNARE Epilog para UNIX y que el agente SNARE para Windows y Lasso pueden recoger los eventos del Controlador de Dominio.

2.4.1 Servidor Splunk y Agentes de SNARE.

Los agentes de SNARE solo presentan la vulnerabilidad de que la versión libre únicamente puede enviar los datos hacia el servidor a través del protocolo UDP, el cual como se planteó al inicio del capítulo es menos seguro en la transmisión de datos por la red. El servidor Splunk es una herramienta muy potente que aunque no sea libre, sus desarrolladores brindan una versión con una licencia libre, cuya restricción es que solamente puede procesar al día 500 Mb de información.

A través de entrevistas a los administradores de red de la UCI se conoció que actualmente en la universidad se genera diariamente más de los 500 Mb de información que puede procesar el servidor Splunk. Debido a esta razón la opción de utilizar los agentes de SNARE para que envíen los eventos hacia el servidor de Splunk no puede ser implantada en la UCI debido a que no seria lo más óptimo ya que se perdería mucha información.

2.4.2 OSSEC.

El sistema OSSEC, el cual cuenta con sus propios clientes para los sistemas operativos Linux y Windows es una herramienta muy potente. El problema a la hora de trabajar con esta herramienta es precisamente la característica que lo distingue de que lleva a cabo un sistema de autenticación entre los agentes y el servidor para que pueda existir comunicación entre ellos. En una red tan grande como la de la UCI es muy tediosa la tarea de que una persona deba ir computadora por computadora adicionándoles a los agentes la clave que se le generó en el servidor. Aunque esta medida le da más seguridad al sistema se necesitaría mucho tiempo y personal para realizar la autenticación para cada computadora que se monitoree, por lo que la tarea es muy larga. Otro problema presente con la utilización de OSSEC es que la autenticación antes mencionada se realiza a través de la dirección IP de la computadora donde esté instalado el agente. En la UCI se le asigna la dirección IP a las computadoras a través del protocolo DHCP, el cual a partir de un servidor posee una lista de direcciones IP las cuales se las va asignando dinámicamente cuando estén libres. Durante este proceso, o por otras causas, las direcciones de las computadoras pueden cambiar, lo cual es una

problemática ya que los agentes de OSSEC en caso de que el IP del host sea modificado pierden la conexión con el servidor, por lo que se debería repetir el proceso de adicionar la PC con el nuevo IP en el servidor, generar la llave para esta y copiarla en el agente. Indudablemente esto incidiría en un gasto de tiempo muy grande ya que son muchas las computadoras que constantemente están cambiando su dirección IP. Por todo lo antes planteado se desecho esta posibilidad.

2.4.3 Syslog-ng como servidor y agente para Linux conjuntamente con Lasso.

La herramienta Syslog-ng puede ser configurada como servidor, aceptando los datos de eventos ocurridos desde otras fuentes. En el archivo de configuración se le pueden definir muchas opciones personalizadas de acuerdo a los intereses de la institución. Entre las ventajas con que cuenta Syslog-ng es que además de UDP, también puede utilizar el protocolo TCP para la transmisión de información por la red encriptando los datos. En el caso de Lasso es una herramienta muy potente y de fácil instalación y configuración, capaz de recopilar los EventLogs de Windows y enviarlos hacia un servidor Syslog-ng. Para las computadoras que trabajan en Linux el propio Syslog-ng se configura para realizar la función de agente, enviando los eventos ocurridos hacia el servidor.

2.4.4 Syslog-ng-Agentes de SNARE.

Dado que el grupo de Intersect Alliance ha desarrollado agentes tanto para Windows como para Linux otra variante pudiera ser tomar como servidor el Syslog-ng con su respectiva configuración para recibir eventos desde los agentes y para las computadoras sobre Linux el propio Syslog-ng configurado para que envíe los eventos hacia el servidor, el agente SNARE para Windows realizaría la función de enviar hacia el servidor Syslog-ng la información generada en las computadoras con Windows como sistema operativo. Los agentes de SNARE para Linux son paquetes "**.rpm**", extensión para las distribuciones de Redhat y Fedora que generalmente son usados para servidores. Debido a que las versiones más utilizadas en la UCI son Debian y Ubuntu se determinó que no se utilizaría este agente. Existe una herramienta que permite convertir paquetes "**.rpm**" a "**.dev**", extensión usada en Debian y Ubuntu pero en el proceso de conversión se pierde información haciendo que el software convertido no funcione del todo bien.

2.5 Solución final.

A partir de las características de la red de la UCI de ser muy grande y que las ventajas de unas herramientas es la desventaja de otras se determinó que se pueden aplicar para la recolección de

eventos dos posibles agentes en el caso de las computadoras con Windows. Ambos agentes también cuentan con la posibilidad de recopilar los eventos del Controlador de Dominio dado que el servidor trabaja sobre la versión Windows Server.

La ventaja del protocolo UDP es la velocidad en la transmisión de los datos por lo cual en redes grandes es más óptimo que utilizar el TCP que es más lento. EL gran número de computadoras en la UCI, principalmente en los laboratorios de docencia, de las que se van a recopilar los logs hace que el servidor constantemente esté muy sobre cargado por los datos que se envían desde los agentes. Debido a esto se determinó utilizar el agente de SNARE, que utiliza el protocolo UDP, en las máquinas de los laboratorios de docencia y aulas que trabajan sobre Windows, y así poder realizar filtrados de aquellos eventos que sean importantes solamente y no todos los que se generan. Para el Controlador de Dominio se determinó utilizar el Lasso ya que recopila todos los eventos y utiliza el protocolo TCP brindando mayor seguridad.

Para las PC que utilizan el sistema operativo Linux se utilizó el Syslog-ng como agente configurado para enviar los datos a través del protocolo UDP ya que son muchas las máquinas que utilizan este sistema operativo, y para el caso del servidor Squid el Epilog para UNIX con el correspondiente módulo para recopilar los logs de Squid. Como servidor se escogió el Syslog-ng con la respectiva configuración para trabajar como servidor. Ver Anexos Figura 23.

Como herramienta para visualizar los datos almacenados en la base de datos, realizar filtrados y otras acciones se determinó utilizar el PHP-Syslog-ng.

2.6 Conclusiones.

En este capítulo se detallaron los protocolos más usados para la transmisión de datos a través de la red, TCP y UDP. Se evidenció que TCP es el más idóneo para la transmisión de los datos por la red si lo que se desea es que viajen seguros, pero en caso de que los intereses se basen en que la transmisión se haga con mayor velocidad se puede utilizar el UDP. Se describieron las herramientas actuales que más potencialidades tienen para ser utilizadas en la UCI para la recolección de los logs así como las posibles soluciones para darle respuesta al problema planteado. Indudablemente el hecho de que la red de la UCI sea tan grande y el protocolo a utilizar por parte del sistema para la transmisión de los datos determinaron la decisión final y más óptima. Como servidor se utilizó Syslog-ng, el cual a su vez será el agente para Linux con la correspondiente configuración, y para Squid se determinó el Epilog para UNIX con el módulo para Squid incluido. Se plantearon dos posibles variantes

para el caso de los agentes para las PC que trabajan sobre Windows: la herramienta Lasso y el agente de SNARE. Con la utilización de Lasso se logrará más fiabilidad en la transmisión de los datos aunque será más lenta debido al uso de TCP, en el caso del agente de SNARE se tendrá mayor velocidad pero menos seguridad por el uso de UDP.

CAPÍTULO 3: INSTALACIÓN Y CONFIGURACIÓN DE LAS HERRAMIENTAS.

3.1 Introducción.

En este capítulo se describirán los pasos para la instalación de los agentes y servidor para la recolección de los eventos. También se especifican las herramientas complementarias que son necesarias instalar para el funcionamiento del servidor.

3.2 Definición de las Áreas de Riesgo.

En la UCI existen niveles de acceso a las distintas computadoras de su red. Hay personas que por cuestiones de trabajo tienen acceso a todas las computadoras de la universidad con permisos de administración, que no son más que los administradores de la red. Además está el grupo de técnicos de laboratorios que por cuestiones de trabajo también tienen privilegios de administración en determinados laboratorios. Lo mismo ocurre con las aulas, donde existe una computadora por cada una de ellas donde solo las personas autorizadas tienen permisos de administración.

Los sistemas para la recolección de eventos cuentan con agentes que se ejecutan como procesos en las computadoras donde se instalan. Cualquier persona que inicie sesión en una computadora con privilegios de administración tiene la posibilidad de detener estos procesos. Debido a ello en aquellas computadoras donde además de los administradores de la red y los técnicos tengan privilegios de administración alguna otra persona no es instalarán los agentes. Por esta razón hay un grupo de computadoras que fueron excluidas de las Áreas de Riesgo, y son las siguientes:

- Apartamentos.
- Laboratorios de producción.
- Oficinas.
- Comedores.

De acuerdo con lo antes expuesto se determinó que los agentes para la recolección y envío de eventos hacia el servidor solamente se instalarán en las siguientes áreas de la UCI, determinándose así que serían las Áreas de Riesgo.:

- Laboratorios de docencia.
- Aulas.

- Servidores centrales de Squid y el Controlador de Dominio.

3.3 Instalación y configuración de las herramientas utilizadas.

A continuación se explicará el proceso de instalación y configuración de las herramientas utilizadas para darle solución al problema planteado.

3.3.1 Instalación del agente de SNARE para Windows.

Los agentes de SNARE para Windows cuentan con una consola para guiar a los usuarios de una manera muy fácil durante el proceso de instalación de la herramienta. El archivo de instalación se puede descargar desde el sitio http://www.intersectalliance.com. Luego de ejecutar dicho archivo se muestra la siguiente ventana donde se inicia la instalación. En dicha ventana se debe dar clic en el botón “Next” o “Siguiente” en español.

Figura 1. Consola de instalación del agente de SNARE.

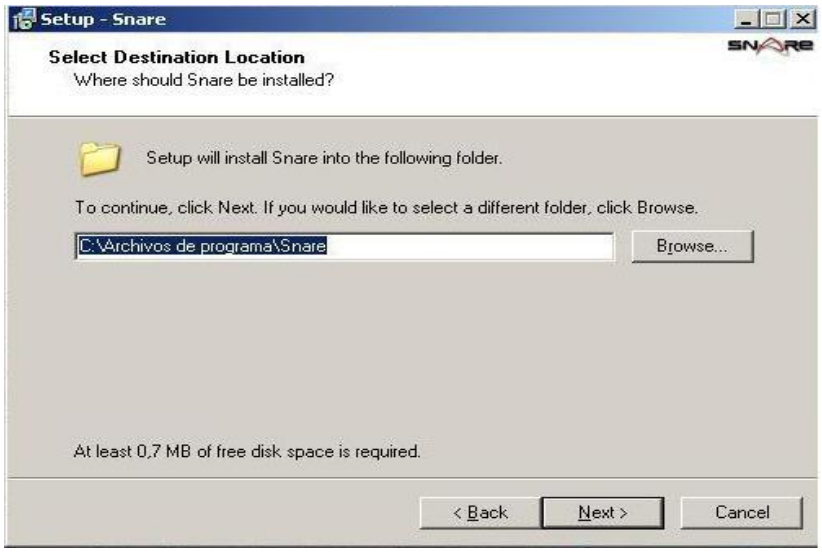

Figura 2. Directorio donde se instalará el agente.

En la Figura 2 se muestra la opción de dónde desea el usuario que se instale el agente de SNARE. Por defecto se realiza en C:\Archivos de programa\Snare pero este directorio puede variar de acuerdo a la decisión del usuario. A través del botón Browse se busca otra dirección en caso deseado.

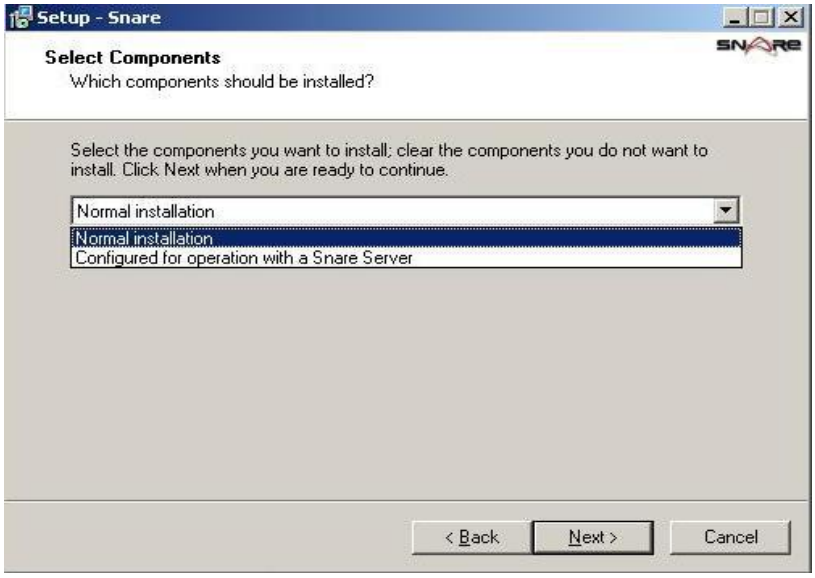

Figura 3. Escoger tipo de instalación.

En esta opción se debe seleccionar “Normal Installation” o “Instalación Normal” debido a que la segunda opción es para aquellos usuarios que hayan comprado el Servidor de SNARE y que el agente enviará hacia este.

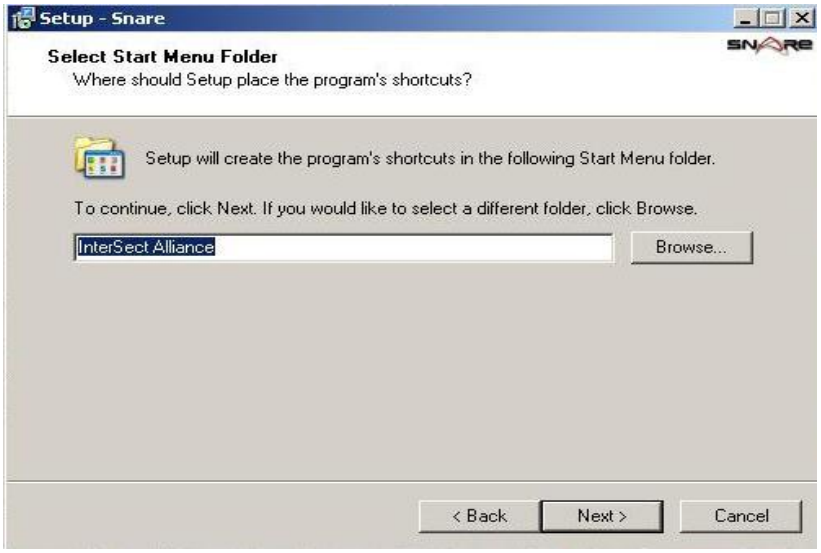

Figura 4. Escribir nombre con el que aparecerá la carpeta en el menú “Inicio”.

Por defecto el nombre con que aparecerá la carpeta en el menú “Inicio” de “InterSect Alliance”, pero puede ser cambiado por el que desee el usuario.

Figura 5. Si se desea o no que el agente de SNARE tome el control de la configuración de los EventLog de Windows.

Esta opción se recomienda que se seleccione “Yes” o “Sí” debido a que permitirá al agente tomar el control de la configuración de auditoria de eventos del sistema, sobrescribiendo estos a partir de su configuración. Dicha configuración puede ser cambiada en la sección “Objectives Configuration”.

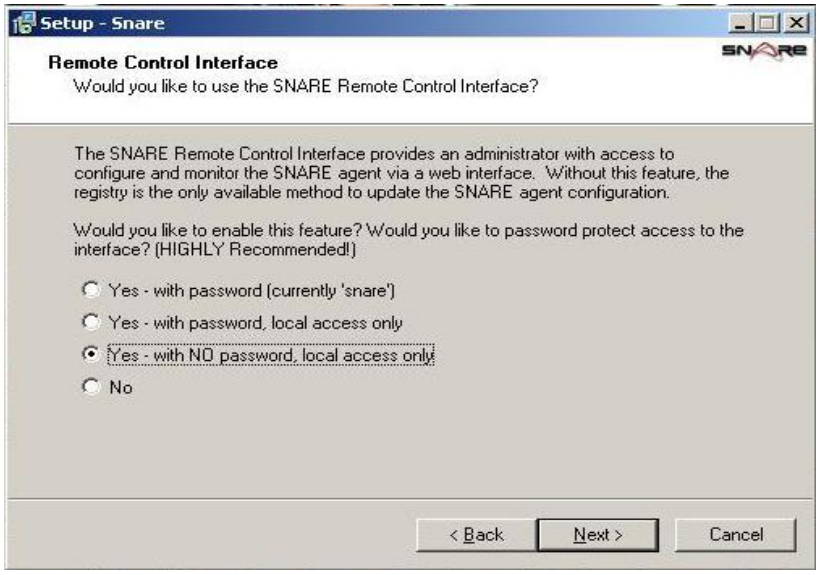

Figura 6. Configuración para el control remoto del agente.

Se puede escoger si se desea o no habilitar la interfaz web así como el acceso remoto al agente dentro de 3 opciones posibles y la 4ta es en caso de que no se desee trabajar con la interfaz web lo cual no es recomendable ya que de ser así solamente a través de los registros se podrá configurar el SNARE.

- **Yes- with password (currently “snare”)**: Habilitar la interfaz web, se desea controlar remotamente el agente y con contraseña que por defecto es “snare”. Se debe escoger esta opción.
- **Yes- with password, local access only**: Habilitar la interfaz web, con contraseña que por defecto es “snare” pero no permite ser controlado remotamente.
- **Yes- with NO password, local access only**: Habilitar la interfaz web, sin contraseña y no permite ser controlado remotamente.
- **NO**: No habilitar la interfaz web.

Luego finaliza el proceso de instalación y se deben realizar determinadas configuraciones en el agente para su correcto funcionamiento.

3.3.2 Configuración del agente de SNARE para Windows.

El agente de SNARE para Windows opera a través de un componente simple, la aplicación base del servicio SnareCore (snarecore.exe). Este servicio interactúa con el subsistema de registro de eventos de Windows para leer, filtrar y enviar los eventos de Aplicación, Sistema o Seguridad hacia un servidor remoto. La interfaz web muestra en la columna izquierda las distintas opciones con que cuenta la herramienta y las distintas configuraciones que se le pueden hacer. Ver Anexos Figura 5.

Current Events: Flujo de Eventos. En esta opción se observan los últimos eventos que han sido filtrados hasta el momento. Ver Anexos Figura 6.

Network Configuration: Configuración de Red. En esta se le configura al agente de SNARE hacia qué servidor enviará los logs definiéndole la dirección IP de este, entre otras opciones. Ver Anexos Figura 7.

- **Override detected DNS Name with**: En este campo se sobrescribe el nombre que se le da al host cuando Windows es instalado. A menos que se requiera de un nombre diferente para ser enviado en el proceso de recogida de eventos de log, este campo se puede dejar en blanco, ya que el servicio de SnareCore usará el nombre que tiene por defecto el host durante la instalación.
- **Destination SNARE Server address**: En este campo se le introduce la dirección de IP del servidor.
- **Destination Port**: Puerto por el que se enviarán los datos hacia el servidor de Syslog-ng. En la investigación se utilizó el propio 6161 que tiene por defecto el agente de SNARE.
- **Use UDP or TCP**: En este campo se selecciona el protocolo por el cual serán enviados los datos, UDP ó TCP. Esta opción no aparece en el agente de SNARE libre debido a que la capacidad de utilizar el protocolo TCP y la posibilidad de enviar eventos a múltiples host está solo disponible para aquellos usuarios que hayan adquirido el servidor de SNARE, de ahí que en este agente la opción de escoger el protocolo no está presente, por lo que por defecto se hace por UDP.

- **Perform a scan of ALL objectives, and display the maximum criticality?**: Esta opción es para si se desea ejecutar un escaneo de todos los objetivos y mostrar los máximos críticos de seguridad. Si se marca esta opción, realizará un escaneo a través de cada objetivo definido y salvará información acerca de los mayores críticos encontrados. El evento será enviado con este valor de crítico. En caso de que esta opción sea desmarcada entonces el evento se enviará tan pronto como sea detectado una amenaza de acuerdo con los objetivos, lo cual puede reducir el consumo de CPU del agente de SNARE, pero los valores de críticos pueden que no sean los más altos.
- **Allow SNARE to automatically set audit configuration? y Allow SNARE to automatically set file audit configuration?**: Si se desea que SNARE automáticamente determine los parámetros necesarios para una auditoría efectiva, se deben marcar las dos opciones. Se recomienda que estos dos parámetros sean marcados porque de no ser así y/ó las ventanas de políticas del grupo de dominio activo sobrescriben la configuración de auditoria, entonces se hace necesario garantizar manualmente que las ventanas de configuración de auditoría sean equivalentes con la configuración de auditoria que se decidió.
- **Export SNARE Log data to a file?**: Esta opción es para si se desea que los logs sean salvados en un lugar determinado.
- **Enable SYSLOG Header?**: Se debe marcar esta opción ya que es el requerimiento para incorporar el encabezado SYSLOG, y enviarlos así hacia un servidor Syslog-ng.
- **SYSLOG Facility:** Facilidad de Syslog. Se debe escoger “Syslog” porque se enviará hacia un servidor Syslog-ng.
- **SYSLOG Priority:** Prioridad Syslog. Se debe escoger “DYNAMIC” para que dinámicamente el agente determine la prioridad de los eventos.

Remote Control Configuration: Configuración de Control Remoto de SNARE. Esta opción constituye uno de los rasgos más significativos de los agentes de SNARE y fue incorporada para permitir que todas las funciones que están disponibles normalmente puedan ser controladas través de un navegador estándar desde otra computadora. Es importante saber que cualquier configuración que se haga vía remota modificará las realizadas manualmente.

- **IP Address allowed to remote control SNARE**: En este campo se le define la dirección IP de la computadora a la que le está permitido realizar las acciones de control remoto.
- **Password to allow remote control of SNARE**: Se le puede poner una contraseña si solo los usuarios autorizados pueden acceder a las funciones de control remoto. Si se accede de forma remota a las funciones de SNARE a través de un buscador el nombre de usuario es “snare” y la contraseña es la que se haya puesto a través de esta configuración.
- **Web Server Port**: Normalmente un servidor web trabaja por el puerto 80. Solo se necesita escribir la dirección en el buscador para acceder al sitio, quedando **http://ip_de_la_pc:puerto_definido**. El puerto que trae por defecto el servidor web del servicio SnareCore es el 6161, el cual puede ser cambiado a través de esta opción si se desea.

Objectives Configuration: Configuración de Objetivos. A través de esta opción se configuran los objetivos de filtrado del agente. Ver Anexos Figura 9.

Es la funcionalidad más importante del agente de SNARE, ya que permite filtrar los eventos. Esto se logra a través de la capacidad de los objetivos de auditoria avanzada. Cualquier número de objetivos pueden ser especificados, los cuales son mostrados en la propia ventana de **Objectives Configuration**. Estos objetivos pueden ser borrados o modificados a partir de los botones de “Delete” ó “Modify” respectivamente. Para adicionar un nuevo objetivo se debe dar clic en el botón “Add” en la parte inferior de la página, luego se mostrará la ventana para la configuración de los objetivos. Ver Anexos Figura 10.

Cada uno de los objetivos provee un gran nivel de control sobre el evento que ha sido seleccionado y reportado. Estos eventos son seleccionados de un grupo de gran nivel de requerimientos y más refinados usando los filtros escogidos.

- **Identify the high level event**: Esta opción es para seleccionar el nivel del evento entre la lista que se muestra:
    1. **Logon or Logoff**: Abrir ó cerrar sesión.
    2. **Access a file or directory**: Acceso a algún fichero o directorio.
    3. **Start or stop a process**: Iniciar o parar un proceso.

4. **Use of user rights**: Uso de los derechos de usuario.
5. **Account administration**: Administración de cuentas.
6. **Change the security policy**: Cambios en las políticas de seguridad.
7. **Restart, shutdown and System**: Reinicio, apagado y sistema.
8. **USB events (currently under development)**: Eventos de USB. Actualmente se encuentra en desarrollo esta opción.
9. **Any event(s)**: Cualquier otro evento.

Estos grupos de eventos se corresponden con los objetivos de seguridad más comunes que se puedan encontrar normalmente. Si se requiere cualquier otro tipo de evento se debe seleccionar la opción de "Any event(s)". De cada uno de los grupos se puede aplicar un nivel de importancia o criticidad: Critical, Priority, Warning, Information y Clear, los cuales se encuentran en la parte inferior de la ventana. Estos niveles permiten al usuario restringir más los objetivos de seguridad y rápidamente identificar la criticidad de un evento, a través de los botones en colores de la parte inferior de la página.

Además de estas opciones existen otras que permiten filtrar aún más los eventos.

- **Select the EventID Match Type:** Permite escoger si se desea "Include" o "Exclude" (Incluir o Excluir respectivamente) mensajes que se correspondan con el objetivo definido.
- **EventID Search Term**: Los eventos tienen un número que lo identifican conocido como "Event ID" o Identificador de Evento. Si se selecciona en la parte superior "Any Event(s)", se puede filtrar por el ID de Evento. Si se desean buscar más de un evento se deben escribir todos los ID separados por comas (,). Si se escribe el caracter "*" se seleccionaran todos los eventos.
- **Select the User Match Type**: Esta opción permite el filtrado a partir del nombre de usuario que genera el evento. Permite escoger si se desea "Include" o "Exclude" (Incluir o Excluir respectivamente) uno o varios nombres de usuarios.

- **User Search Term**: En este campo se escribe el nombre o los nombres separados por comas de los usuarios que se desean buscar los eventos. Si se desea que busque de todos se puede poner el caracter (*).
- **Identify the event types to be captured**: Esta opción permite escoger el tipo de eventos que serán capturados dentro del siguiente grupo:
    1. **Success Audit**: Auditoría Exitosa.
    2. **Failure Audit**: Auditoría Fallida.
    3. **Information**: Información.
    4. **Warning**: Advertencia.
    5. **Error**: Error.
- **Identify the event logs (ignored if any objective other than 'Any event(s)' is selected)**: Opción para identificar qué eventos de Windows serán filtrados: Security, System, Application, Directory Service, DNS Server o File Replication. Es importante saber que si en la primera opción se seleccionó cualquier nivel de evento que no fuese “Any Events(s)” se ignorará esta opción. Si se desea que solamente se recopilen los eventos de Seguridad se debe marcar la opción “Security”.
- **Select the Alert Level**: Permite la selección del Nivel de Alerta: Critical, Priority, Warning, Information, Clear. Por ese mismo orden Crítico, Prioridad, Advertencia, Información y Limpio.

Luego de terminar la configuración se debe dar clic en el botón “Change Configuration”.

View Audit Service Status: Ver el Estado del Servicio de Auditoría. Para ver el estado en que se encuentra el agente, si está trabajando o detenido.

Apply the Latest Audit Configuration: Aplicar la Ultima Configuración de Auditoría. Esta opción permite actualizar el servicio con la nueva configuración.

El servicio de SnareCore además tiene la habilidad de recuperar los usuarios locales y del dominio, grupos de usuarios de la computadora donde está instalado el agente y del dominio del que es miembro esta PC, la copia en memoria de los registro. Toda computadora donde esté corriendo el agente de SNARE debe ser miembro de un dominio, y tiene la habilidad para leer información de los usuarios y grupos. Estas funciones se encuentran en la parte inferior izquierda de la página.

- **Local Users**: Usuarios locales de la máquina.
- **Doamin Users**: Usuarios del dominio al que pertenece la PC.
- **Local Group Members**: Grupos de usuarios locales.
- **Domain Group Members**: Grupos de usuarios del dominio.

Registry Dump: Configuración de los usuarios de la máquina.

3.3.3 Instalación del Agente Lasso.

El proceso de instalación de la herramienta Lasso es bastante fácil. Para ello cuenta con una consola de instalación paso a paso. El archivo de instalación se puede descargar desde la dirección http://sourceforge.net/project/showfiles.php?group_id=167062e

Luego de ejecutar el archivo de instalación se mostrará una consola que guía al usuario durante el proceso de instalación:

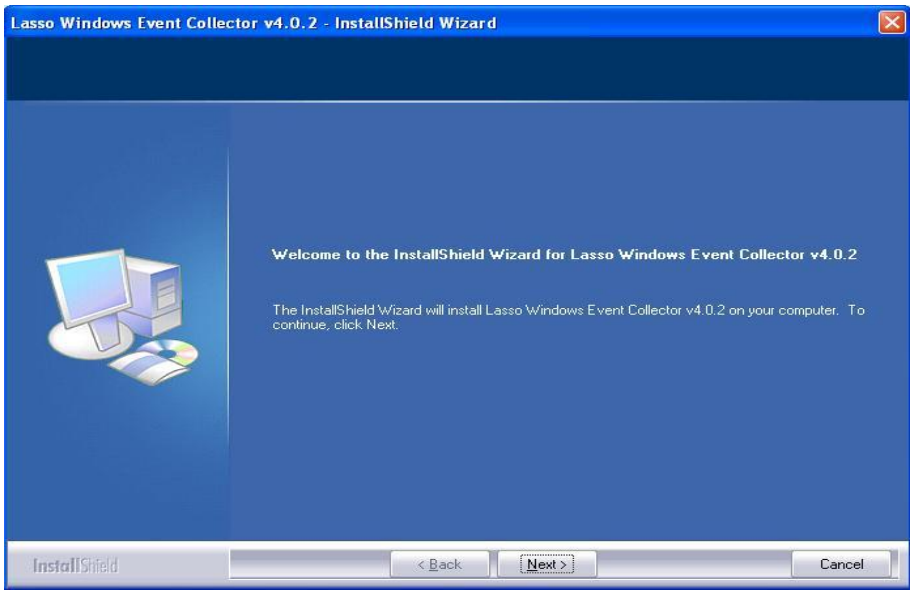

Figura 15. Consola de instalación de la herramienta Lasso.

Pulsar en “Next” para continuar.

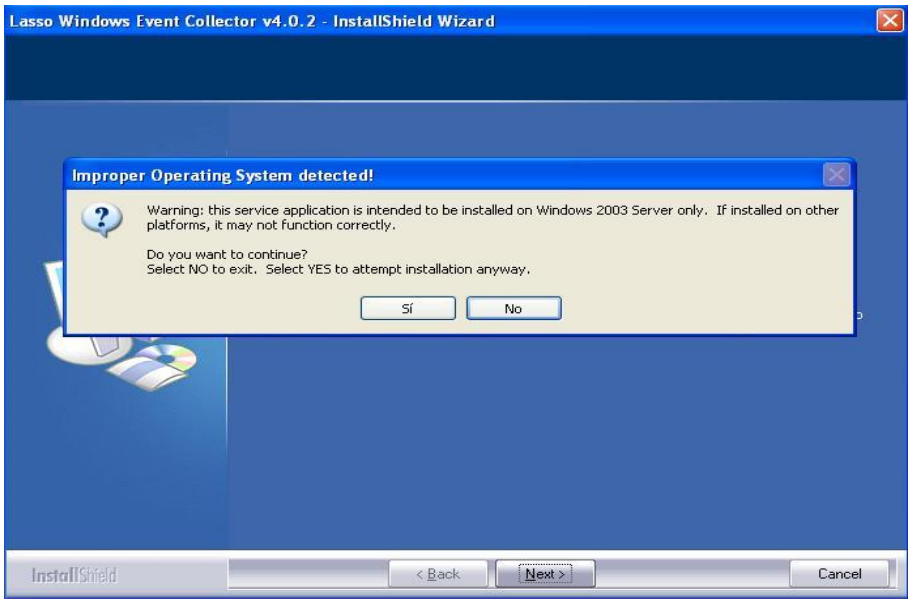

Figura 16. Instalando Lasso.

La herramienta Lasso inicialmente fue desarrollada para trabajar sobre el sistema operativo Windows Server 2003. Si se está instalando en otra versión de Windows, se mostrará una alerta preguntando al usuario si desea continuar con la instalación pese a que no sea Windows Server 2003. Se debe seleccionar “Sí” debido a que este agente trabaja también sobre las otras versiones de Windows.

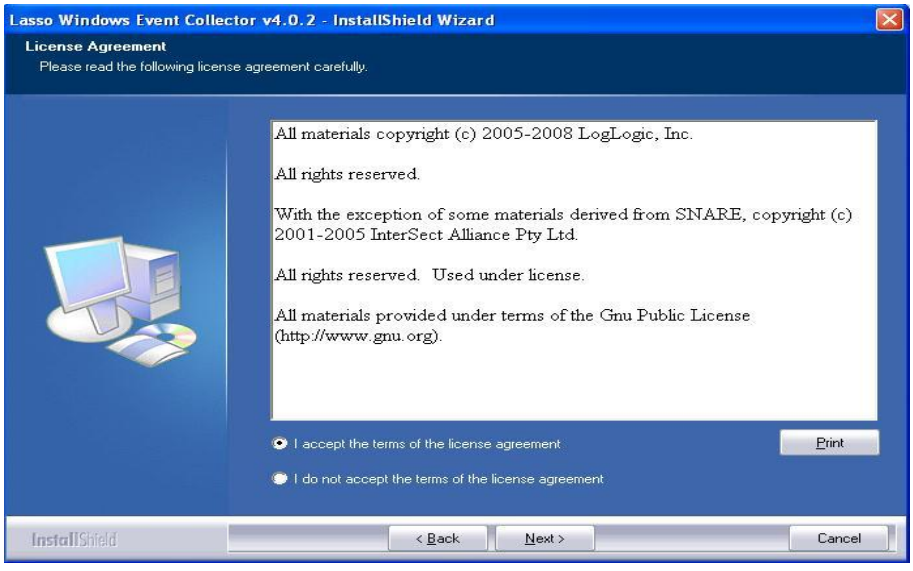

Figura 17. Términos de uso de Lasso.

Se deben aceptar los términos para poder instalarlo.

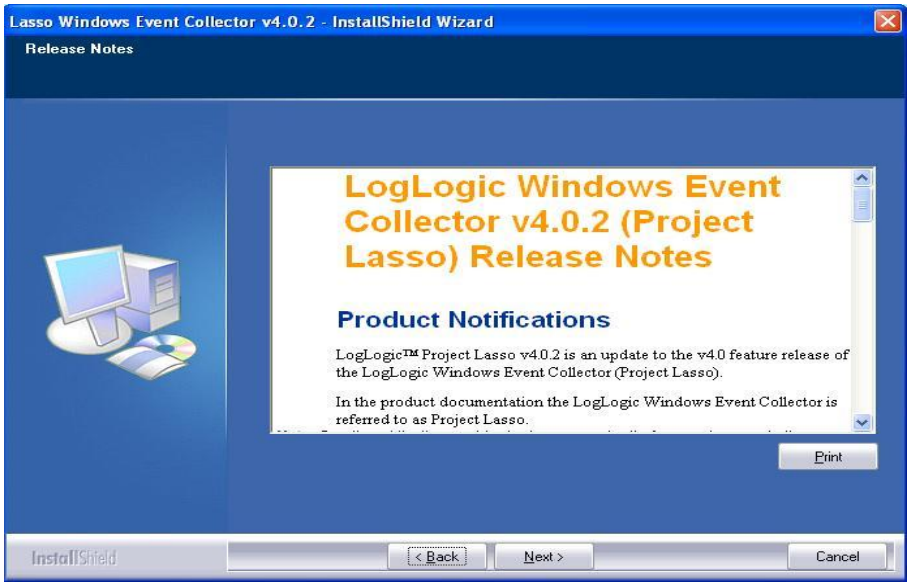

Figura 18. Datos sobre Lasso.

Esta ventana muestra información acerca del grupo desarrollador y la herramienta. Se debe escoger "Next" para continuar la instalación.

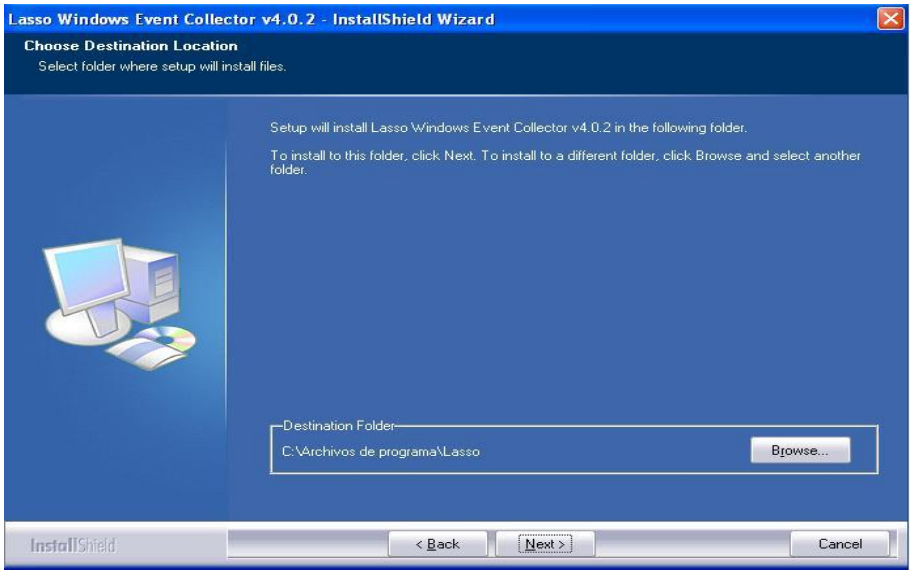

Figura 19. Selección de la carpeta donde se instalará Lasso.

Por defecto Lasso se instalará en **C:\Archivos de Programa\Lasso**. Si se desea que lo haga en otra dirección se debe dar clic en “Browse” y buscar la localización deseada.

Figura 20. Escoger el archivo de configuración.

Si ya se tiene el archivo de configuración en algún directorio se le puede dar la dirección donde se encuentra este para tomar dicha configuración.

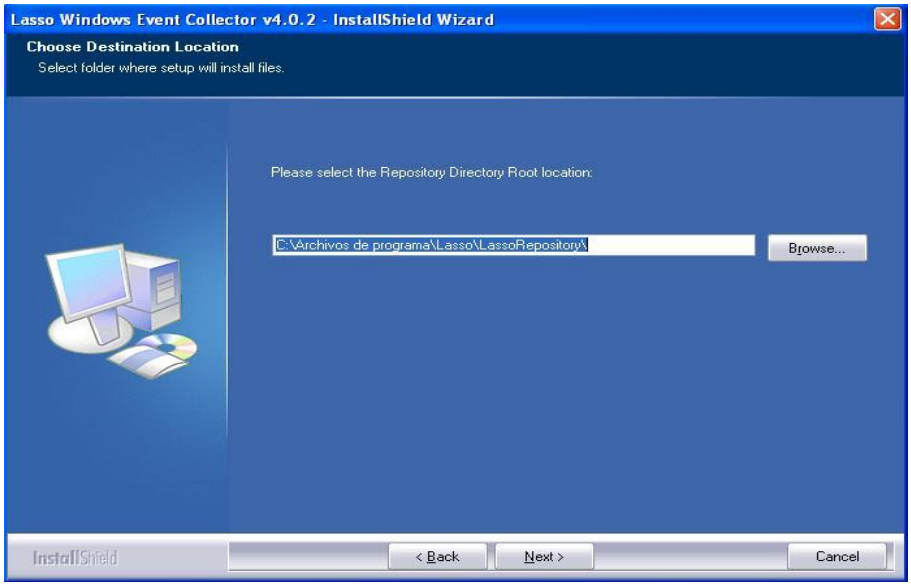

Figura 21. Carpetas donde se instalará Lasso.

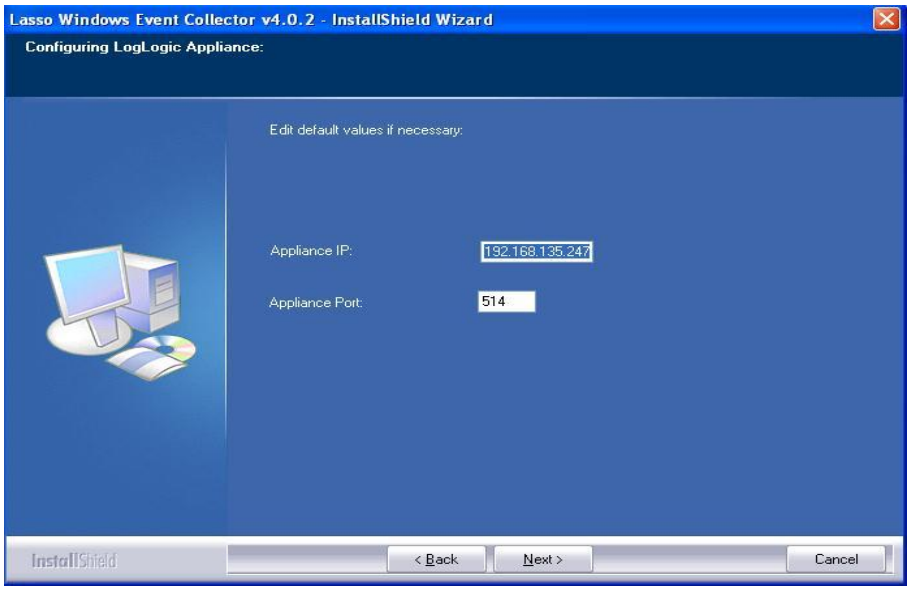

Figura 22. Dirección IP y puerto del servidor de Syslog-ng.

La dirección y puerto del servidor hacia donde enviará Lasso se pueden dejar los que trae por defecto y luego cambiarlos en el archivo de configuración.

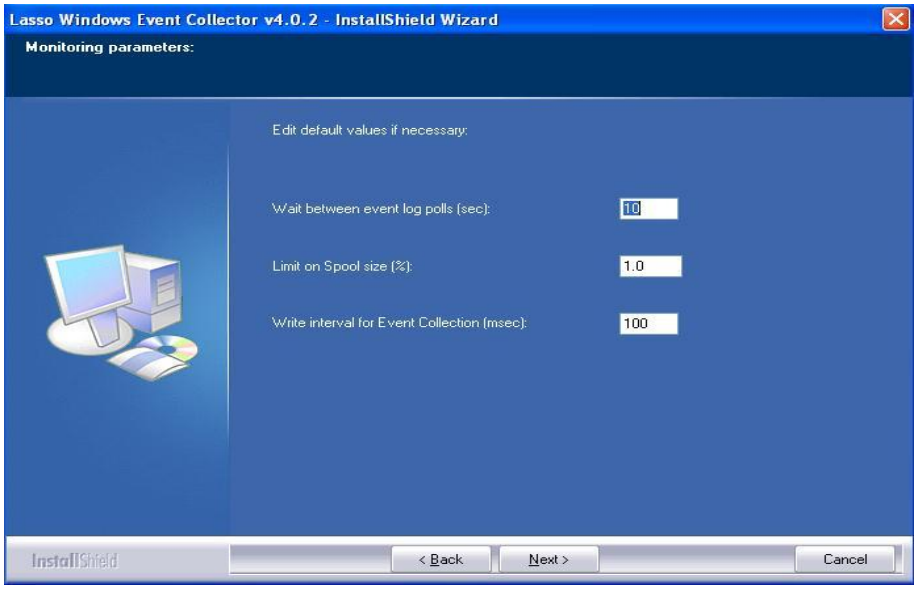

Figura 23. Otras opciones en la configuración de Lasso.

- **Wait between event log polls (sec)**: Intervalo de tiempo en que Lasso verifica la ocurrencia de nuevos eventos.

- **Limit on Spool size (%)**: Límite del tamaño del Spool en porciento.
- **Write interval for Event Collection (msec)**: El intervalo de escritura para la recolección de eventos.

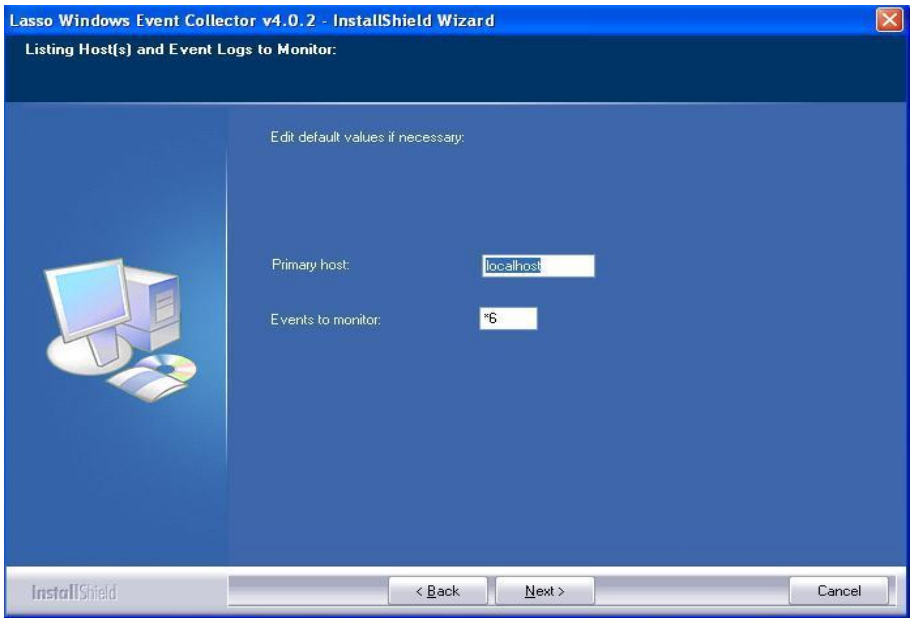

Figura 24. Otras configuraciones de Lasso.

En la Figura 24 se muestran 2 opciones que se deben configurar o dejar los valores que trae por defecto.

- **Primary Host**: Lasso puede recoger los logs de varias computadoras a la vez. Se recomienda que se recojan solamente los de la PC donde esté instalado, por esta razón se le debe dejar el valor que tiene por defecto “localhost”.
- **Events to monitor**: En este campo se le definen los logs que recogerá Lasso. Por defecto tiene el valor “*6”, lo cual significa que recogerá todos los eventos de Windows. Si se desea que solamente recoja los principales, Security, Aplication y System, se debe introducir el valor “*3”, si se desea solamente recoger alguno de estos se debe especificar con los nombre antes mencionado separados por comas (,).

Así se termina la configuración de Lasso en su instalación. Se deber dar clic en el botón “Next” hasta que se termine el proceso.

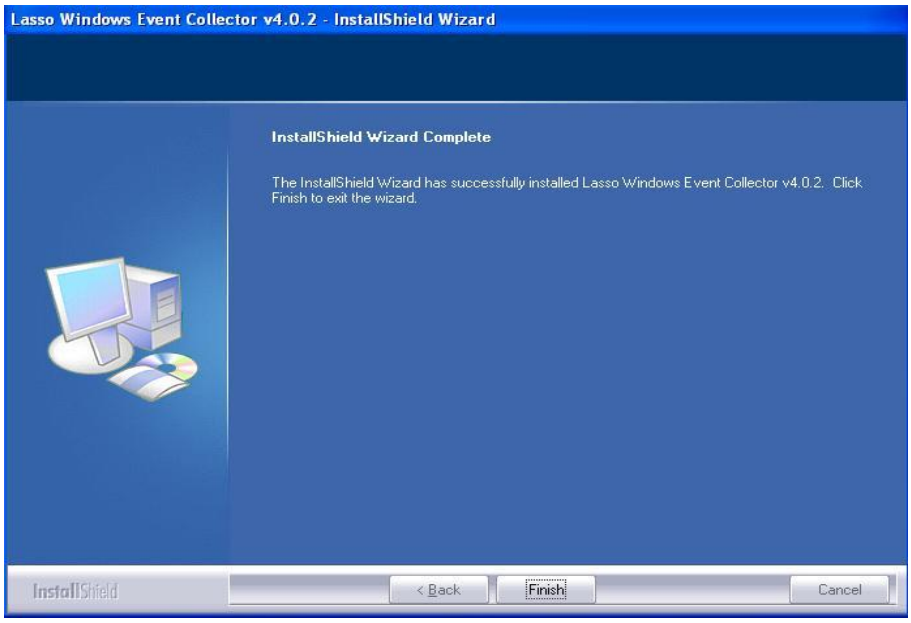

Figura 25. Fin de la instalación de Lasso.

3.3.4 Configuración de Lasso.

Los valores introducidos durante el proceso de instalación de Lasso pueden ser modificados en dos archivos de configuración. Estos archivos se encuentran en **C:\Archivos de programa\Lasso\lasso.ini** y **C:\Archivos de programa\Lasso\hostlist.ini**.

Configuración de lasso.ini.

- LogAppliance: En esta opción se introduce el IP del servidor y el puerto por el que recibirá los mensajes quedando por ejemplo para el IP 10.31.20.180 y el puerto 5800 de la siguiente forma: **LogAppliance,10.31.20.180,5800.**
- EventPollInterval: Se configura el intervalo de tiempo que demorará Lasso en verificar la existencia de nuevos eventos. Ejemplo: **EventPollInterval,1.**

Configuración de hostlist.ini

Solamente se configuran las computadoras de las que recogerá los eventos Lasso, que como se decía anteriormente en este caso solo recogerán los de la PC donde está instalado, y los eventos que serán recopilados. Ejemplo: **localhost,*6**. Los valores posibles son los que se explicaban anteriormente en la Figura 24.

3.3.5 Instalación de SNARE Epilog para UNIX.

El Epilog para UNIX incluye un script que permite la instalación y configuración fácilmente de los componentes principales. Estos componentes son:

- El binario de **Epilog** que contiene el demonio "Epilog" y las funciones principales de SNARE: leer los logs de los ficheros, filtrar los eventos de acuerdo con los objetivos definidos por el usuario, proporciona una interfaz web de control y especifica los logs a monitorear.
- Ficheros de configuración necesarios para permitir al Epilog trabajar con los logs que soporta.
- El script de instalación, **install.sh**, el cual instala todos los componentes necesarios.
- Un script de eliminación, **uninstall.sh**, que permite eliminar todos los componentes de Epilog del sistema.

Los pasos para la instalación son:

1. Descargar el Epilog desde el sitio http://www.intersectalliance.com.
2. Descomprimir el fichero.
3. Moverse hasta la carpeta a través del comando # **cd Epilog**.
4. Desde la consola con el usuario root ejecutar '**./install.sh**'. Con este comando se instala el Epilog.
5. Una vez terminada la instalación el demonio Epilog se iniciará automáticamente.

Para que los eventos sean enviados hacia el servidor, el demonio Epilog debe estar ejecutándose, para ello cuenta con opciones de pararlo, iniciarlo y reiniciarlo a través de los comandos: '**/etc/init.d/epilogd stop**', '**/etc/init.d/epilogd start**' y '**/etc/init.d/epilogd restart**' respectivamente.

Epilog para UNIX cuenta con una interfaz web que permite su fácil configuración. Ver Anexos Figura 1. Esta interfaz se asemeja mucho a la del agente de SNARE para Windows y se puede acceder a ella a través de la dirección **http://localhost:6162**. Solamente algunas opciones presentan particularidades debido a que se monitorean otros tipos de logs.

3.3.5.1 Instalación de SNARESquid.

SNARESquid incluye un script que permite instalar y configurar los componentes. Los principales componentes son:

- Ficheros de configuración que permiten al SNARESquid trabajar con los ficheros logs recibidos.
- Un script de instalación, "**snaresquid_install.sh**".
- Un script para eliminar los componentes SNARESquid del sistema, "**snaresquid_uninstall.sh**".

Para instalar el paquete SNARESquid para UNIX se debe:

1. Verificar que el SNARE Epilog está correctamente instalado.
2. Descargar el "SNARESquid" desde el sitio http://www.intersectalliance.com.
3. Descomprimir el archivo descargado.
4. Moverse hasta la carpeta a través del comando "cd", Ejemplo: **# cd SNARESquid-<versión>**.
5. Ejecutar el fichero de instalación desde la consola como usuario "root": '**./snaresquid_install.sh**'.
6. Una vez instalado el demonio SNARESquid iniciará automáticamente.

El demonio SNARESquid puede ser parado, iniciado o reiniciado a través de los comandos: '**/etc/init.d/snaresquidd stop**', '**/etc/init.d/snaresquidd start**' o '**/etc/init.d/snaresquidd restart**', respectivamente. Por defecto el demonio SNARESquid puede ser controlado a través de la interfaz web de Epilog, sin embargo se puede controlar individualmente. Si en el archivo de configuración **/etc/snare/epilog/squid.conf** está habilitada la opción de control remoto entonces el subsistema SNARESquid puede ser accedido remotamente a través de un navegador web. La siguiente configuración habilita dicha opción donde se define al menos "1" máquina para controlar remotamente el agente, el puerto, el IP de esta máquina y la contraseña si se desea, que se almacena de forma encriptada (el usuario siempre es "snare"):

[Remote]

allow=1

listen_port=6163

restrict_ip=10.0.0.1

accesskey=SnYLb.gT4Gk2k

La dirección para acceder remotamente quedaría: **http://<ip del host>:6163**.

3.3.6 Configuración de Epilog.

Los ficheros de configuración de Epilog se encuentran almacenados en la dirección: **/etc/snare/epilog**, donde están contenidos todos los detalles requeridos por el demonio para ejecutarse exitosamente. En caso de realizar una configuración incorrecta no impedirá la ejecución del sistema pero los logs puede que no sean procesados o enviados hacia el servidor. Independientemente de esto la forma más efectiva y simple de configurar el Epilog es a través de la interfaz web con que cuenta, todo lo que se haga sobre esta se actualizará en el archivo de configuración.

- **Switch Configuration Files**: Cambiar el Fichero de Configuración. Con esta opción se pueden acceder a los archivos de configuración de Epilog y SNARESquid a través de la web. En dependencia de la configuración escogida será como funcione la interfaz. Ver Anexos Figura 11.
- **Log Configuration**: Configuración de los logs a monitorear. Ver Anexos Figura 2. A partir de esta opción se puede adicionar, borrar o modificar el monitoreo de los logs. Luego de pulsar en el botón “ADD” se mostrarán los campos a llenar: La dirección de los ficheros que se van a monitorear y Tipos de logs que serán monitoreados. En la opción “Log File” se debe definir la dirección del fichero de logs que será monitoreado. SNARE Epilog constantemente verificará la ocurrencia de cualquier cambio en el fichero, e inmediatamente reportará hacia el servidor. Aunque el fichero sea rotado, reemplazado o borrado, el Epilog continuará supervisando dicho fichero y en caso de ser borrado esperará hasta que sea creado y continuar su trabajo normalmente. En la opción “Log Type” se debe introducir el tipo de logs. Los tipos de logs disponibles son:

    1. **GenericLog** -- Formato de logs Genérico (por defecto).
    2. **ApacheLog** -- Logs web de Apache.
    3. **ISAWebLog** – Logs web de ISA.
    4. **MSProxySvr** – Logs del servidor proxy de Microsoft.
    5. **SMTPSvcLog** – Logs de SMTP.
    6. **SquidProxyLog** – Logs del Proxy Squid.

- **Network Configuration**: En el caso de la configuración de la red el Epilog para UNIX presenta algunas diferencias con respecto al agente de SNARE para Windows. Los campos principales que se deben llenar en esta opción son: el nombre del host donde está instalado el Epilog, dirección IP del servidor y puerto por el que se enviarán los datos hacia este. En el caso del nombre del host si no se introduce ninguno el Epilog tomará el que tiene la PC por defecto. Al igual que todos los agentes que ha desarrollado el grupo Intersect Alliance, el Epilog para UNIX tiene las restricciones de que las opciones de usar el protocolo TCP y enviar los datos hacia múltiples servidores solamente está disponible para los usuarios que hayan comprado el servidor de SNARE con los respectivos agentes. Las opciones de **SYSLOG Priority y SYSLOG Facility** son las mismas que las que presenta el Agente de SNARE para Windows. Ver Anexos Figura 4.
- **Remote Control Configuration, View Audit Service Status y Apply the Latest Audit Configuration**: Las opciones Configuración de Control Remoto, Ver Estado del Servicio de Auditoría y Aplicar la Última Configuración de Auditoría se configuran y realizan las mismas acciones que en los agentes de SNARE para Windows anteriormente explicado.

Objectives Configuration: La principal ventaja de los agentes de SNARE es la posibilidad que brindan de filtrar los eventos. El Epilog para UNIX cuenta con esta característica también. Por defecto no está definido ningún objetivo y por consiguiente todos los eventos serán enviados hacia el servidor. Debido a cuestiones de seguridad y que se deben conocer todas los eventos ocurridos en el servidor proxy Squid se debe trabajar con esta configuración. Ver Anexos Figura 3. En caso de necesitar algún tipo de filtrado el SNARESquid brinda la posibilidad de realizarlos a partir de expresiones regulares. Para ello se debe pulsar en el botón “Add” y se mostrarán las opciones. Ver Anexos Figura 12.

3.3.7 Requisitos de Hardware para el servidor.

Debido a la gran cantidad de computadoras que constantemente enviarán datos hacia el servidor, el volumen de información será muy grande por lo que la máquina del servidor deberá contar con determinados requisitos para su correcto funcionamiento. El principal requisito es el espacio de almacenamiento ya que a partir de pruebas realizadas en el laboratorio se comprobó que el volumen diario de información aproximadamente en las posibles 2000 PC y servidores donde se montarán los agentes sería de 20 Gb diario.

Pentium 4.

3 Gb de RAM.

800Gb - 1 Tb de Disco Duro.

3.3.8 Paquetes que deben ser instalados en el servidor.

Antes de la instalación de Syslog-ng se deben instalar algunos paquetes que son necesarios para su funcionamiento. Como sistema operativo se utilizó Ubuntu 7.10 con escritorio GNOME y se utilizó el gestor de paquetes Synaptic (se puede acceder en Sistema-Administración-Gestor de Paquetes Synaptic). Los necesarios son:

- MySQL-server 5 (Gestor de Base Datos).
- Apache2. (Servicio Web).
- php5 (lenguaje de programación Web).
- Phpmyadmin. (Cliente para administrar el gestor de Base Datos)
- Syslog-ng.

3.3.9 Instalación del servidor Syslog-ng.

La instalación del Syslog-ng se hizo desde el repositorio para Ubuntu 7.10 que tiene la UCI. A partir de esto se puede hacer de dos formas. Es importante saber que cualquiera de las vías que se utilice para instalar Syslog-ng automáticamente eliminará el Syslogd que tiene por defecto el sistema operativo y que se deben tener privilegios de “root”.

1. Utilizando el gestor de paquetes Synaptic: La herramienta Synaptic se instala por defecto con el sistema operativo Ubuntu 7.10, la cual es usada para la instalación y desinstalación de paquetes. Utilizando este programa la instalación es muy fácil, esta muestra todos los paquetes disponibles en el Repositorio, donde se debe escoger Syslog-ng e instalar.
2. Utilizando la consola Prompt: A través de la consola Prompt se pueden realizar prácticamente todas las tareas en una computadora a través de comandos. Para instalar Syslog-ng se debe ejecutar el comando: ***apt-get install Syslog-ng***.

3.3.10 Configuración del servidor Syslog-ng.

Luego de la instalación del Syslog-ng se deben realizar un grupo de configuraciones en el archivo de configuración del Syslog–ng ubicado en la dirección **/etc/syslog-ng/syslog-ng.conf**. Este archivo se

divide en cinco partes fundamentales: Options, Source, Destination, Filter, Log Paths. Dentro de estos grupos se introducen determinadas configuraciones necesarias para el funcionamiento del servidor.

Options: "Opciones". Este grupo contiene las opciones más globales para el funcionamiento general del servidor Syslog-ng. La sintaxis es la siguiente, donde "**params**" se refiere a parámetros que son pasados a las opciones "**option**":

options { option1(params); option2(params); ... };

Ver Anexos Figura 18.

Source: "Fuentes". Las fuentes son una colección de drivers que recolectan los mensajes usando un método dado. La sintaxis de las fuentes es el siguiente, donde "**identifier**" es el nombre que tendrá la fuente definida, "**source-driver**" es el manejador de fuente y "**params**" es el parámetro que se le pasa a este manejador:

source <identifier> {source-driver (params);

source-driver (params); ...

};

Ver Anexos Figura 19.

Destination: "Destino". El destino es donde los logs son enviados si cumplen con las reglas de filtrado. Al igual que las fuentes, están compuestos por uno o más drivers, cada uno definiendo como los mensajes serán manejados. La sintaxis para hacer un destino es la siguiente, donde "**identifier**" es el nombre que se le da al identificador, "**destination-driver**" es el nombre del manejador del destino, al cual se le pasan parámetros a través de la variable "**params**":

destination <identifier> {

destination-driver(params);
destination-driver(params); ... };

Ver Anexos Figura 20.

Filter: "Filtros". Los filtros controlan en enrutamiento de los logs dentro del Syslog-ng. Se pueden escribir expresiones "booleanas", las cuales pueden contener operadores "**and**", "**or**" y "**not**", y un

mensaje pasa si la expresión es verdadera. Syslog-ng cuenta con varias opciones para realizar el filtrado:

- **facility**: Filtrar los eventos que tengan determinada facilidad.
- **level() or priority()**: Filtrar los eventos que tengan determinada prioridad.
- **program()**: Usando expresiones regulares permite filtrar logs que contengan el nombre de algún programa.
- **host()**: Permite filtrar eventos de determinado host usando expresiones regulares.
- **match()**: Filtrar logs que cumplan con determinada expresión regular.
- **filter()**: Llamar a otra regla de filtrado.
- **netmask()**: Filtra las PC que pertenecen a una determinada subred.

La sintaxis de los filtros es, donde "**identifier**" es el nombre que se le da al filtro y "**espression**" es una expresión booleana que puede contener además de "**and**", "**or**" y "**not**" las opciones antes mencionadas:

filter <identifier> { expression; };

Ver Anexos Figura 21.

Log Paths: "Camino de los logs". Los grupos anteriores deben ser conectados. En este grupo se declaran dichas conexiones, así cualquier mensaje que proviene de alguna de las fuentes y pasa todos los filtros es enviado hacia los destinos. Se puede hacer un "Camino de Logs" con la siguiente sintaxis, donde está compuesto por fuentes "**source**", filtros "**filter**", destinos "**destination**" e indicadores o "**flags**", los cuales pueden cambiar el comportamiento que tiene por defecto las demás opciones:

log { source(s1); source(s2); ...

filter(f1); filter(f2); ...

destination(d1); destination(d2); ...

flags(flag1[, flag2...]); };

Ver Anexos Figura 22.

Una vez configurado el servidor se debe generar la base de datos, para ello con la herramienta Phpmyadmin se debe importar el sript “syslog.sql” lo cual contienen las instrucciones para generar la base de datos con todas las tablas que la conforman. Luego se deben hacer configuraciones en el arranque del servidor Syslog-ng para ello se abre el fichero **/etc/init.d/syslog-ng** y debajo de la línea **PATH=/sbin:/bin:/usr/sbin:/usr/bin** se debe copiar lo siguiente:

```
LD_LIBRARY_PATH=/usr/local/lib/
export LD_LIBRARY_PATH

/root/syslog-mysql-pipe.sh & INIT_NAME=`basename "$INIT_PROG"`
```

Estas líneas ejecutarán el fichero llamado **“syslog-mysql-pipe.sh”** que debe crearse en el directorio **/root**. Para crear dicho fichero se debe dar permiso de escritura a la carpeta **root** a través del comando **$cd /root $chmod -R 777 ./**. En la configuración se debe especificar el usuario y contraseña para conectarse a la base de datos:

```
#!/bin/bash
if [ -e /var/log/mysql.pipe ]; then

while [ -e /var/log/mysql.pipe ]

do
mysql -u usuarioBD --password=passwordparausuarioBD syslog < /var/log/mysql.pipe

done

else

mkfifo /var/log/mysql.pipe

fi
```

Después se debe dar permiso al fichero de la siguiente forma: **$chmod 700 /root/syslog-mysql-pipe.sh.** De esta forma se garantiza que cada vez que se inicie el servicio se cree el fichero “mysql.pipe” y comienza la escritura en la base de Datos a través de la “tubería” “mysql.pipe”.

3.3.11 Configuración del Syslog-ng como agente.

Luego de la instalación del Syslog-ng, explicada anteriormente, se deben introducir algunas instrucciones, al igual que en el servidor, en el archivo de configuración para que envíe los registros

eventos hacia el servidor Syslog-ng. En este caso en el grupo “Destination” se especifica la dirección y el puerto del servidor Syslog-ng.

Options.

Source.

Destination.

Log Path.

Ver Anexos Figura 23.

3.3.12 Configuración de PHP-Syslog-ng.

PHP-Syslog-ng constituye una facilidad desarrollada para visualizar los datos recopilados por Syslog-ng. Permite realizar filtrados y búsquedas a partir de criterios como el nombre o IP de la PC, la Facilidad, Prioridad o fecha de los registros de eventos, así como ordenarlos por fecha, Prioridad entre otros. Ver Anexos Figura 13.

Con el objetivo de sobrecargar menos el servidor y por cuestiones de seguridad se debe instalar el PHP-Syslog-ng en otro servidor, como puede ser un servidor de aplicaciones. Para ello se necesitan instalar en este servidor las siguientes herramientas:

- Apache2. (Servicio Web): se debe adicionar el puerto 5800 en el archivo de configuración que es el utilizado por PHP-Syslog-ng.
- php5 (lenguaje de programación Web).

Una vez descargado el paquete de la dirección:

http://sourceforge.net/project/downloading.php?group_id=68685&use_mirror=ufpr&filename=phpsyslogng-2.8.tar.gz&5545878 se deben seguir los siguientes pasos:

- Descompactar el paquete.
- Copiar la carpeta descompactada en la carpeta **/var/wwww**.
- Se buscan las siguientes líneas en el fichero **/var/www/phpsyslogng/config/config.php**:

  // DBUSER is the name of the basic user.

  define('DBUSER', 'usuarioBD');

// DBUSERPW is DBUSER's database password.

define('DBUSERPW', 'passwordparausuarioBD');

// DBHOST is the host where the MySQL server is running.

define('DBHOST', 'direccion_server');

Donde **'usuarioBD'** y **'passwordparausuarioBD'** corresponden al usuario y contraseña que debe definir el usuario para que la aplicación se conecte a la base de datos. En **'direccion_server'** se debe introducir la dirección del servidor Syslog-ng, donde mismo se encuentra la base de datos.

- Acceder a la dirección **http://localhost/phpsyslogng/index.php**, la página principal de PHP-Syslog-ng. Para loguearse por primera vez el usuario y el password es "admin", una vez logueado se puede cambiar la contraseña y crear nuevos usuarios. También se puede acceder desde otra PC a través de la dirección **http://10.31.20.180:5800/phpsyslogng/index.php**.

3.3.13 Opciones de PHP-Syslog-ng.

Logout: "Desloguear". Esta opción es para si se desea cerrar la sesión actual.

Search: "Buscar". "Search" es la facilidad principal que presenta PHP-Syslog-ng debido a que es donde se pueden realizar los filtrados y búsquedas dentro de los registros de eventos recopilados en la base de datos por el Syslog-ng. Para ello cuenta con varias opciones que se describen a continuación.

- **Host**: Permite escoger si se desea "Include" o "Exclude" (Incluir o Excluir respectivamente) algún host para el filtrado.
- **Syslog Facility**: Permite escoger si se desea "Include" o "Exclude" (Incluir o Excluir respectivamente) alguna Facilidad para el filtrado.
- **Syslog Priority**: Permite escoger si se desea "Include" o "Exclude" (Incluir o Excluir respectivamente) alguna Prioridad para realizar el filtrado.
- **Date** y **Time**: Intervalos de Fecha y Hora en que se desea realizar una búsqueda.
- **Records Per Page**: Esta opción permite escoger la cantidad de registros de eventos que se mostraran en una página.

- **Order By**: Criterio a escoger para ordenar los logs mostrados. Entre estos están por fecha, Prioridad, entre otros.
- **Search Order**: Orden en que se desea que se muestren los resultados de la búsqueda: “DESC” o “ASC”, Descendente o Ascendente respectivamente.
- **Search Message**: Otra de las posibilidades que brinda PHP-Syslog-ng es filtrar a partir de mensajes. Por defecto los mensajes definidos en los 3 campos debajo de esta opción son incluidos en la búsqueda, si se marca la opción “Exclude” en alguno de ellos será excluido.
- **Collapse Identical Messages Into One Line**: Si se marca esta opción los mensajes que sean iguales serán mostrados en una sola línea.

Config: “Configuración”. La opción “Config” permite administrar las cuentas y privilegios para el acceso a la página. Para ello cuenta con las opciones de crear y eliminar usuario, cambiar contraseña y privilegios a algún usuario. Ver Anexos Figura 14.

Help: “Ayuda”. La opción “Help”, al igual que casi todo el software que se desarrollan en el mundo cuenta con información que ayudan al usuario a trabajar con la herramienta.

About: “Acerca de”. Esta opción brinda información acerca del grupo desarrollador y la herramienta.

3.4 Conclusiones.

En este capítulo se describió el proceso de instalación, configuración así como las opciones de las herramientas utilizadas para dar solución al problema. Evidentemente se deben tener conocimientos básicos del sistema operativo Linux además de Windows para instalar y configurar dichas herramientas.

CONCLUSIONES

- En la investigación se evidenció la importancia que tienen los logs de eventos para mantener la seguridad de una red.
- Se han desarrollado muchas herramientas, cada una con sus peculiaridades, pero en general tienen como objetivo principal la centralización de los registros de eventos.
- Luego de tener los logs de las computadoras y servidores que forman parte de una red almacenados en un servidor central es mucho más fácil su procesamiento, humanizando y agilizando el trabajo de los administradores de red.
- Se llegó a la solución para el problema planteado a través de herramientas totalmente libres.

RECOMENDACIONES

- Continuar la investigación sobre el tema de la centralización de logs por la importancia que estos tienen para la seguridad de una PC y la red completa como tal.
- Implementar un sistema que a partir de los logs recopilados por el servidor Syslog-ng sea capaz de procesar estos profundamente con el objetivo de detectar posibles acciones malignas y enviar las alertas correspondientes.
- Debido a que la el volumen de información recibido en el servidor es muy grande se recomienda realizar Backups de la base de datos.
- Monitorear los procesos de los agentes para en caso de estar inactivos sean activados lo antes posible.

REFERENCIAS BIBLIOGRÁFICAS

(Raiden, 2008): **RaidenFTPD TEAM. 2002.** ¿Cómo puedo usar el nombre automático de log y cual es el formato del archivo de log? *RaidenFTPD.* [Online] 2002. [Cited: Enero 15, 2008.] http://www.raidenftpd.com/en/raiden-ftpd-doc/spanish/formatolog.htm.

(GFI, 2008): **—. 2006.** GFI EventsManager descubre qué está realmente ocurriendo en su red. *GFI.* [Online] Octubre 12, 2006. [Cited: Enero 22, 2008.] http://www.gfi.com/news/es/esmlaunch.htm.

(Barcelona/04 Computing Group, 2004): **Barcelona/04 Computing Group. 2004.** *El nuevo Applications Agent consolida logs con cualquier formato.* [Documento] Barcelona, España : s.n., Marzo 2004.

(EHAS, 2004): **Joaquin. 2004.** EHAS. *EHAS.* [Online] 2004. [Cited: Marzo 25, 2008.] http://interno.ehas.org/intranet/organizacion/nuevo-wiki/Gesti_c3_b3nDeRedes

(Coutin, et al., 2003): **Coutin, Adrian and Valdés, Mirta. 2003.** *Estudio de las estadísticas Web de accesos y visitas del Portal Cuba.cu.* [Documento PDF.] Ciudad de la Habana, Cuba : s.n., 2003.

(Equipo de GNU, 2008): **Equipo de GNU. 2008.** La Definición de Software Libre. *El Sistema Operativo GNU.* [En línea] 21 de Abril de 2008. http://www.gnu.org/philosophy/free-sw.es.html.

BIBLIOGRAFÍA

Baluja García, Walter and Curbelo Pruna, Maykel. 2004. *Sistema Analizador de Log para la Detección de Intrusos.* [Power Point] Ciudad de la Habana, Cuba : s.n., Mayo 2004.

Barcelona/04 Computing Group. 2004. *El nuevo Applications Agent consolida logs con cualquier formato.* [Documento] Barcelona, España : s.n., Marzo 2004.

BRconnection. 2008. OSSEC Frequently Asked Questions. *Ossec.* [Online] 2008. [Cited: Marzo 22, 2008.] http://www.ossec.net/wiki/index.php/FAQ.

—. 2007. OSSEC Manual. *OSSEC.* [Online] 2007. http://www.ossec.net/main/manual/.

Campin dot Net. 2008. Syslog-ng FAQ. *Campin dot Net.* [Online] Enero 16, 2008. [Cited: Marzo 17, 2008.] http://www.campin.net/syslog-ng/faq.html.

Coutin, Adrian and Valdés, Mirta. 2003. *Estudio de las estadísticas Web de accesos y visitas del Portal Cuba.cu.* [Documento PDF.] Ciudad de la Habana, Cuba : s.n., 2003.

Dunston, Duane. 2008. Centralized File-Integrity With Samhain Part I. *LinuxSecurity.* [Online] 2008. http://www.linuxsecurity.com/content/view/117702/171/.

EHAS. 2004. Gestión de redes. *EHAS.* [Online] 2004. [Cited: Marzo 25, 2008.] http://interno.ehas.org/intranet/organizacion/nuevo-wiki/Gesti_c3_b3nDeRedes.

GFI. 2006. GFI EventsManager descubre qué está realmente ocurriendo en su red. *GFI.* [Online] Octubre 12, 2006. [Cited: Enero 22, 2008.] http://www.gfi.com/news/es/esmlaunch.htm.

Giovanni Zuccardi, Juan David Gutérrez. 2006. *Informática Forense.* [Documento PDF.] 2006.

Intersect Alliance. 2007. Resources. *Intersect Alliance.* [Online] 2007. [Cited: Enero 12, 2008.] http://www.intersectalliance.com/resources.

LogForge. 2008. LogForge. *LogLogic.* [Online] 2008. [Cited: Febrero 15, 2008.] http://www.loglogic.com/logforge/.

Niño Mejía, Diana Carolina and Sierra Múnera, Alejandro. 2007. *CENTRALIZACIÓN DE REGISTROS DE EVENTOS.* [Documento PDF.] Bogotá, Colombia : Pontificia Universidad Javeriana., Enero 11, 2007.

BIBLIOGRAFÍA.

NSF grant (NCR-9796082). 2008. About Squid. *Squid-cache.org.* [Online] 2008. [Cited: Enero 15, 2008.] http://www.squid-cache.org/.

NTP community. 2007. NTP: The Network Time Protocol. *Welcome to ntp.org, home of the Network Time Protocol project.* [Online] Julio 2007. [Cited: Enero 18, 2008.] http://www.ntp.org/.

RaidenFTPD TEAM. 2002. ¿Cómo puedo usar el nombre automático de log y cual es el formato del archivo de log? *RaidenFTPD.* [Online] 2002. [Cited: Enero 15, 2008.] http://www.raidenftpd.com/en/raiden-ftpd-doc/spanish/formatolog.htm.

Scheidler, Balázs. 2006. Syslog-ng v1.6 reference manual. *Liberalia Tempus.* [Online] Agosto 25, 2006. http://www.liberaliatempus.com/syslog-ng_reference_manual_v16.html.

Softpedia. 2008. GFI EventsManager description. *Softpedia.* [Online] 2008. [Cited: Enero 15, 2008.] http://www.softpedia.com/get/System/System-Info/GFI-EventsManager.shtml.

Splunk. 2005. Documentation. *Splunk.* [Online] 2005. [Cited: Enero 12, 2008.] http://www.splunk.com/doc/latest/.

Equipo de GNU. 2008. La Definición de Software Libre. *El Sistema Operativo GNU.* [En línea] 21 de Abril de 2008. http://www.gnu.org/philosophy/free-sw.es.html.

Walter Baluja García, Maykel Curbelo Pruna. 2003. *Sistema Analizador de Log para la Detección de Intrusos.* [Power Point] Ciudad Habana : s.n., 2003.

ANEXOS

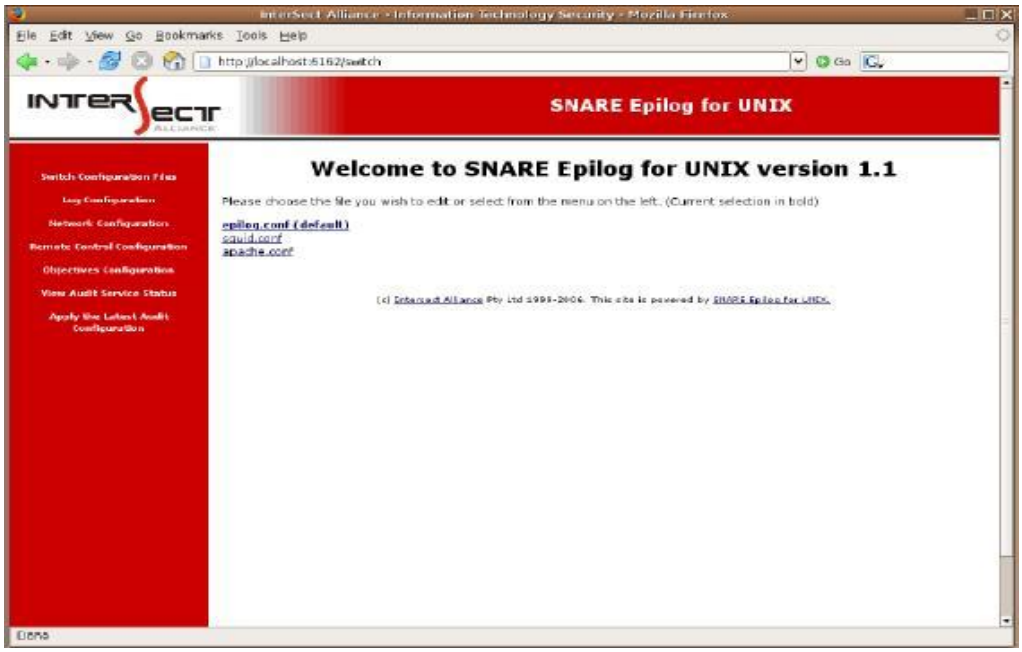

Figura 1. Interfaz web del SNARE Epilog para UNIX.

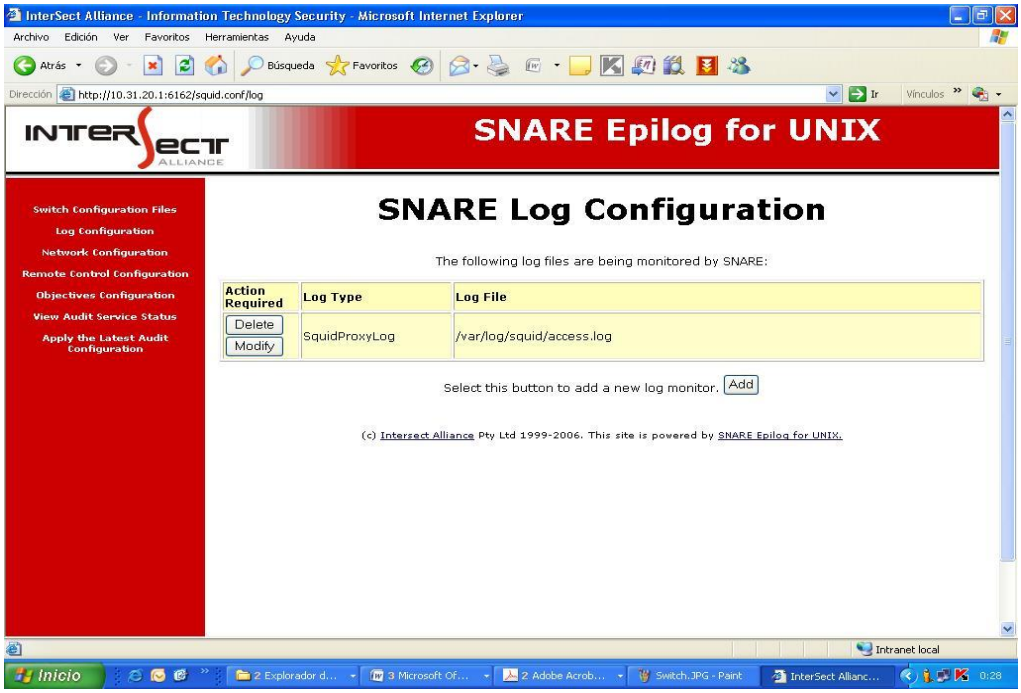

Figura 2. Configuración de Log del Epilog.

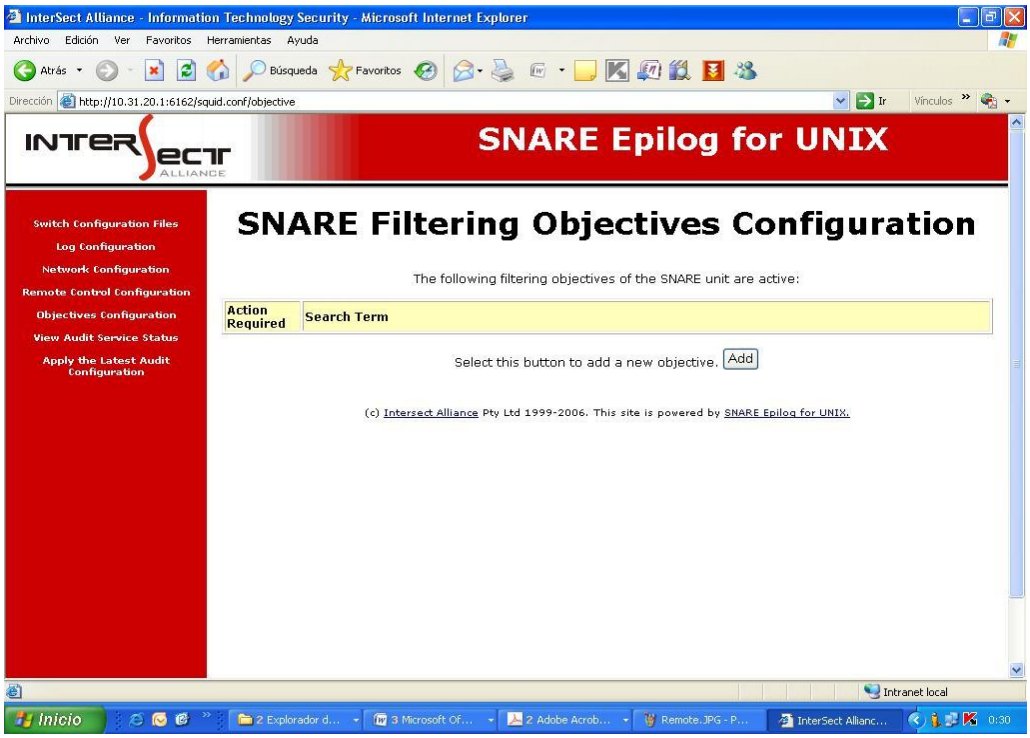

Figura 3. Configuración de los Objetivos de Filtrado del Epilog para UNIX.

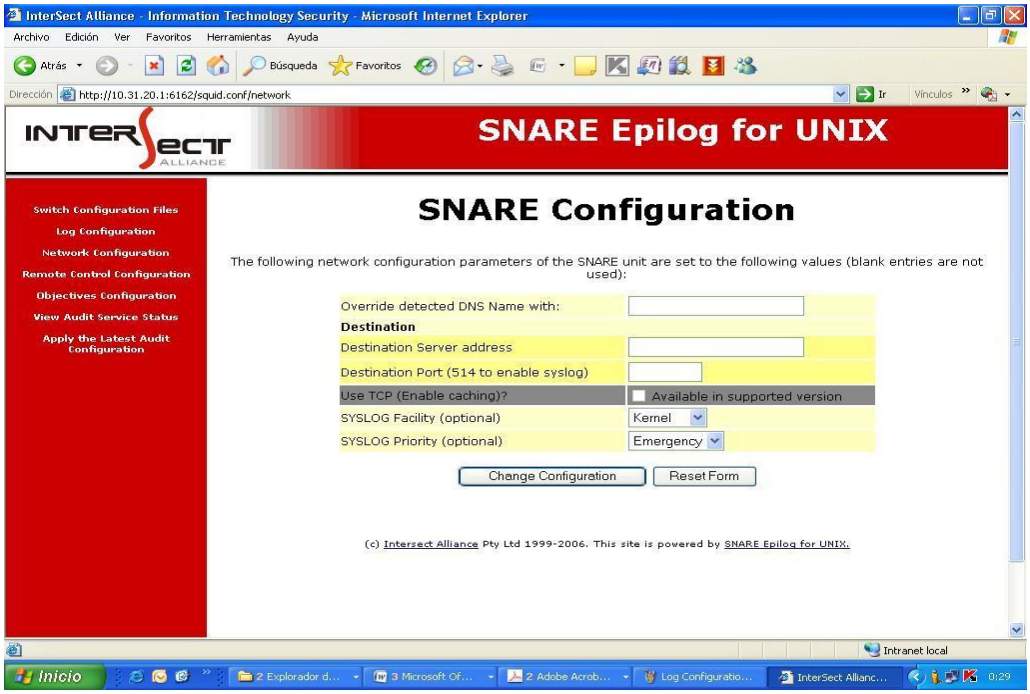

Figura 4. Configuración de la red del Epilog para UNIX.

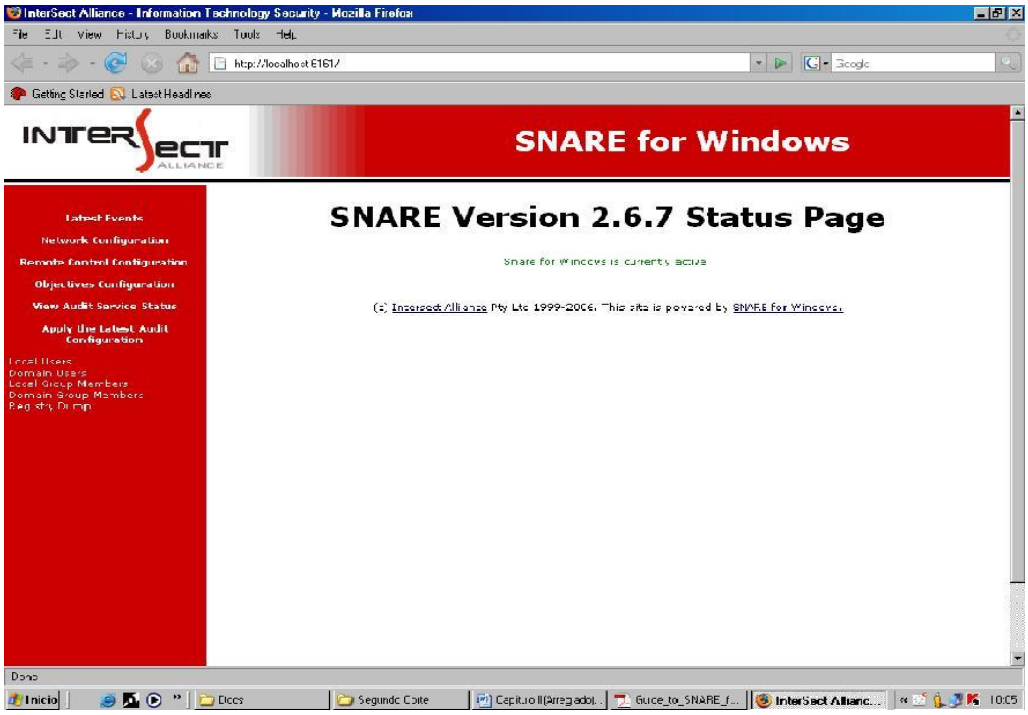

Figura 5. Interfaz Web del agente de SNARE para Windows.

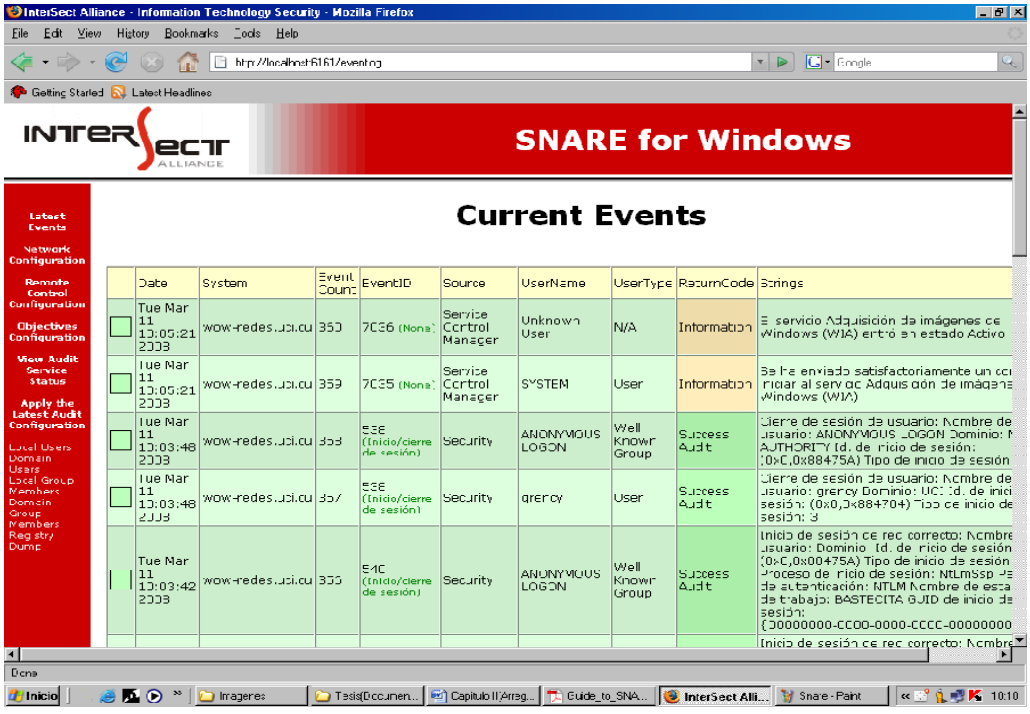

Figura 6. Últimos registros de eventos capturados por el agente de SNARE para Windows.

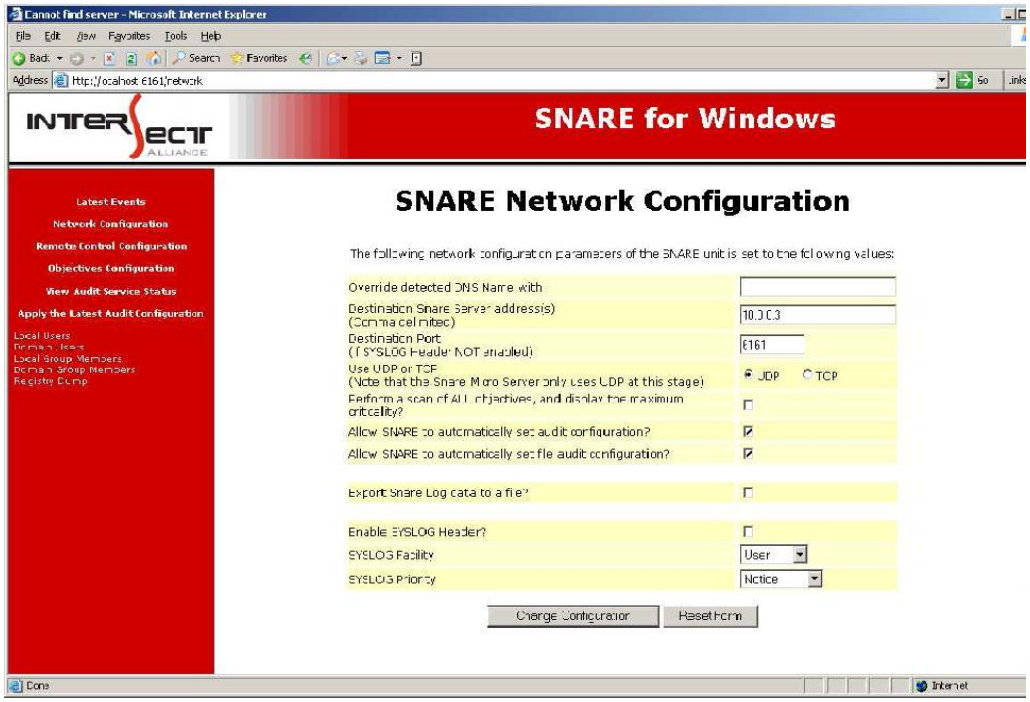

Figura 7. Configuración de la red del agente de SNARE para Windows.

Figura 8. Configuración para controlar remotamente el agente de SNARE.

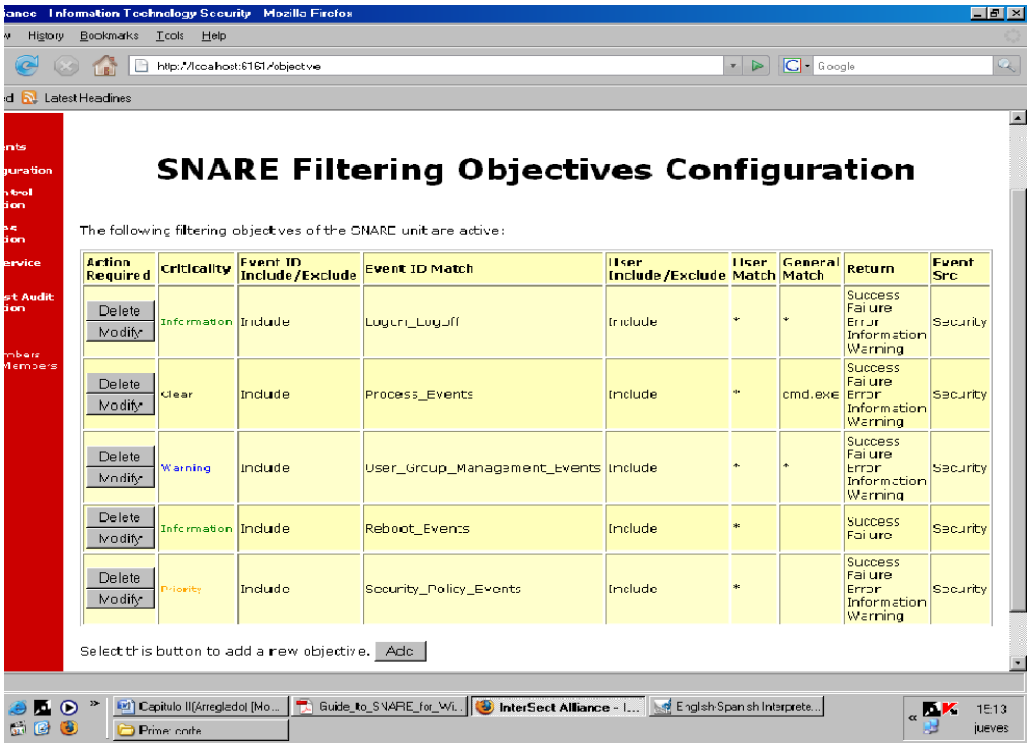

Figura 9. Objetivos para el filtrado de los logs en el agente de SNARE.

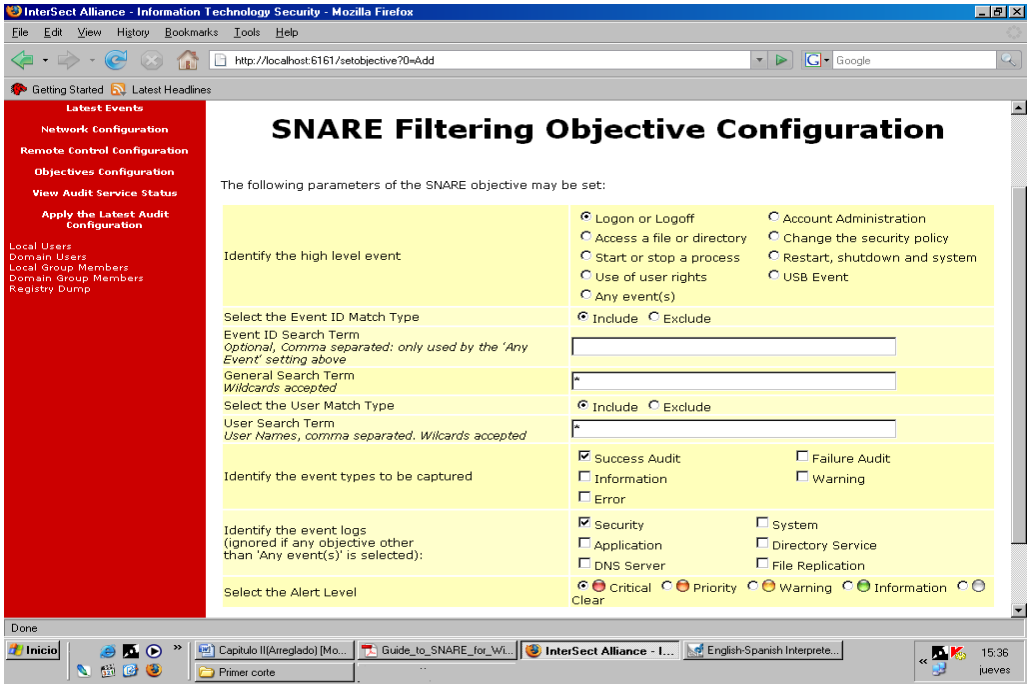

Figura 10. Creación o modificación de un objetivo en el agente de SNARE.

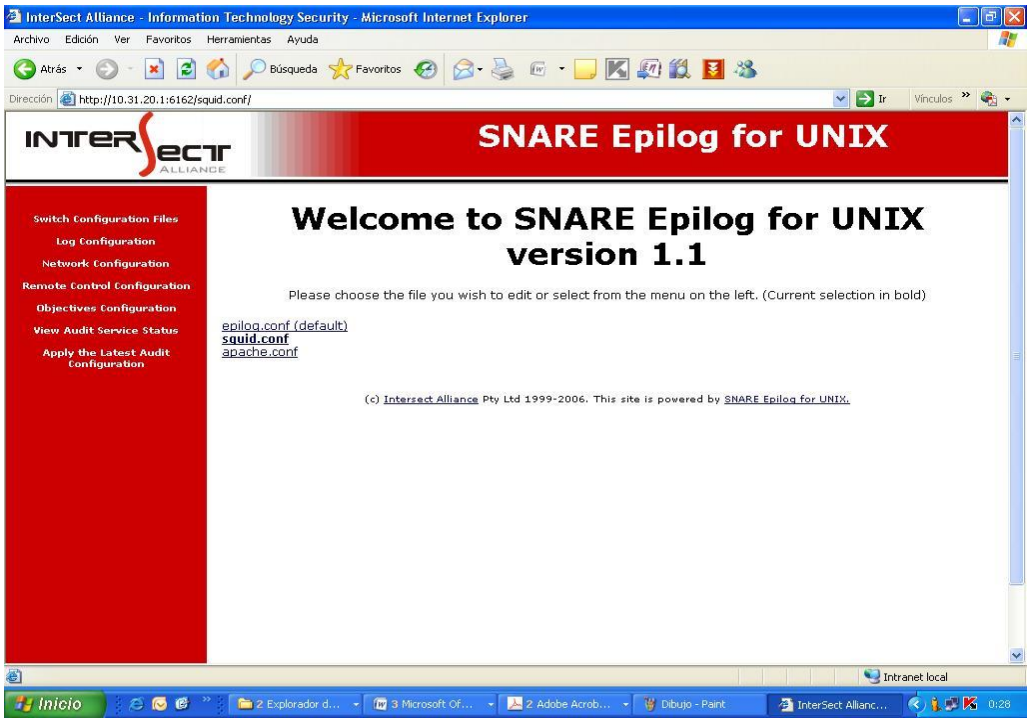

Figura 11. Selección de la configuración en Epilog para UNIX.

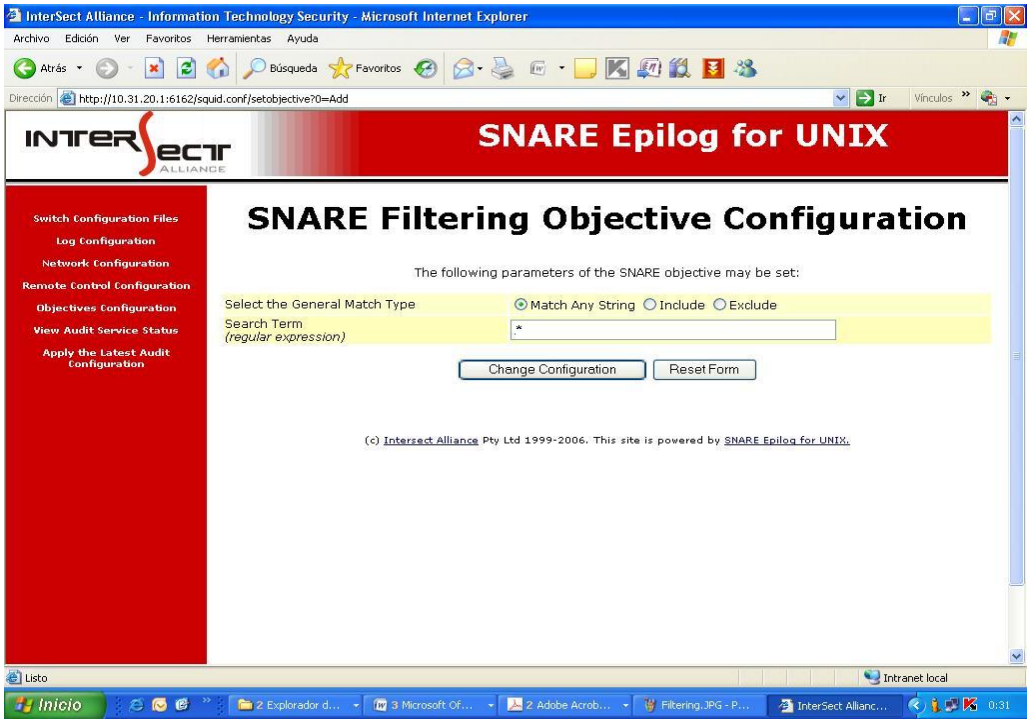

Figura 12. Filtrado a partir de expresiones regulares en Epilog para UNIX.

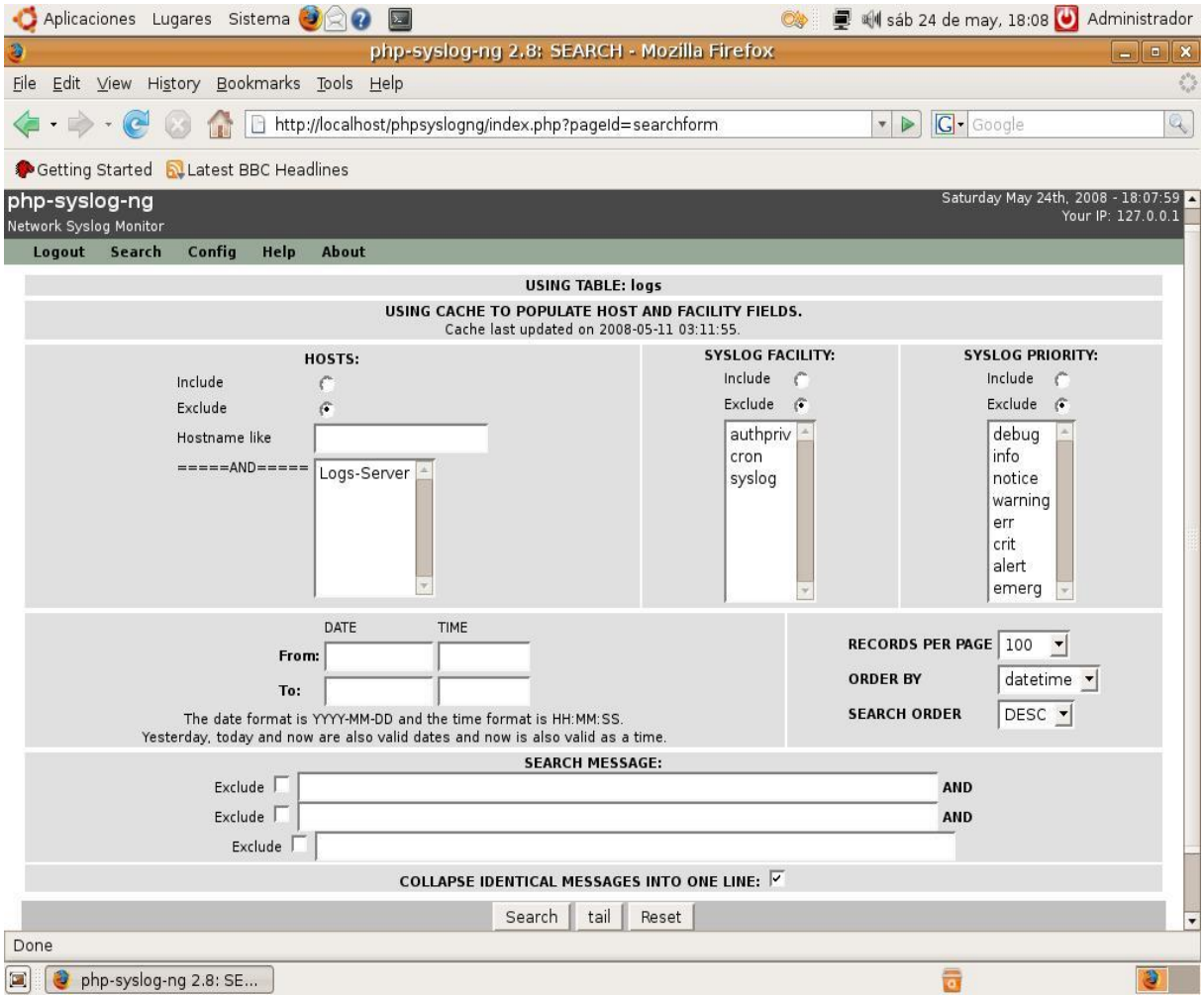

Figura 13. Opciones de búsqueda y filtrado en PHP-Syslog-ng.

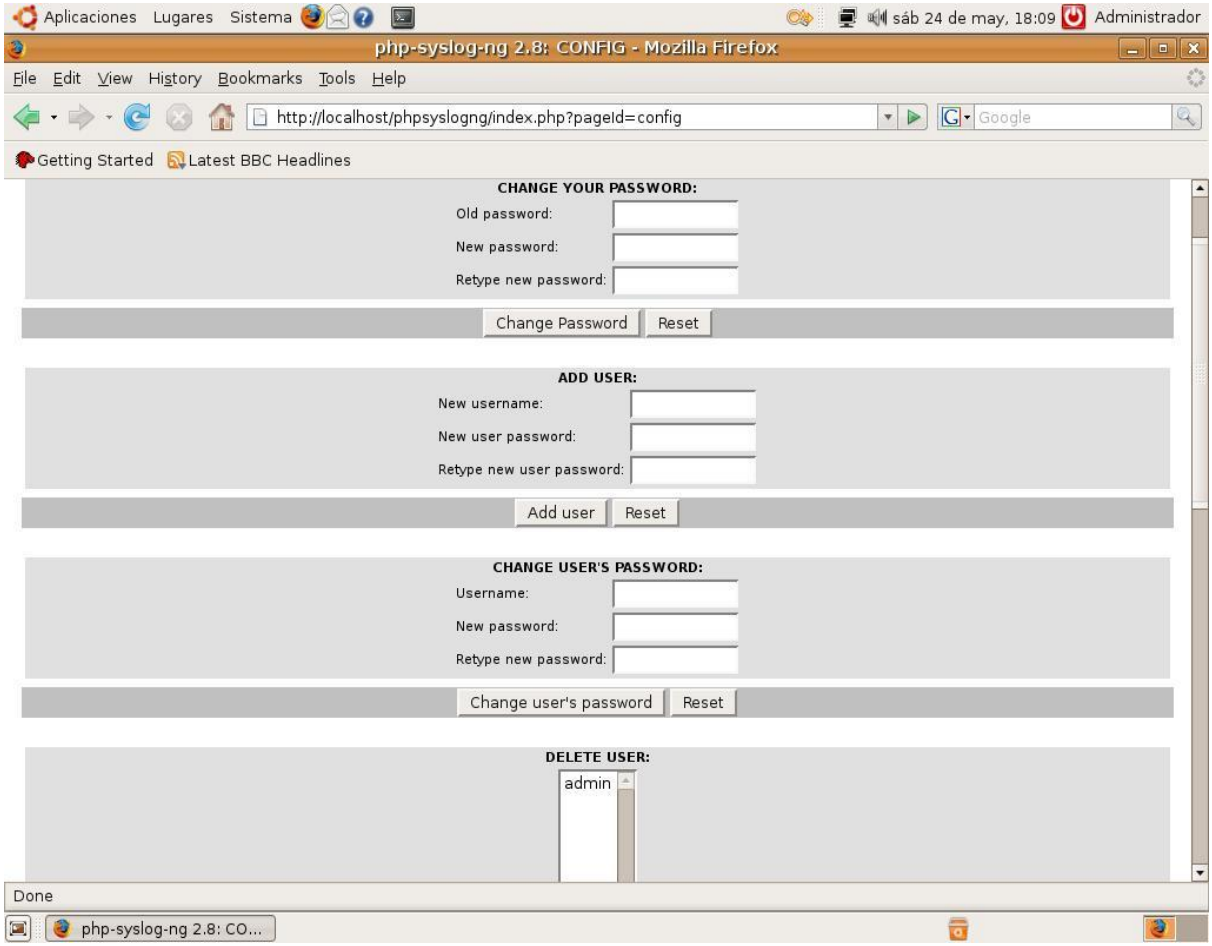

Figura 14. Administración de cuentas y privilegios para el acceso a PHP-Syslog-ng.

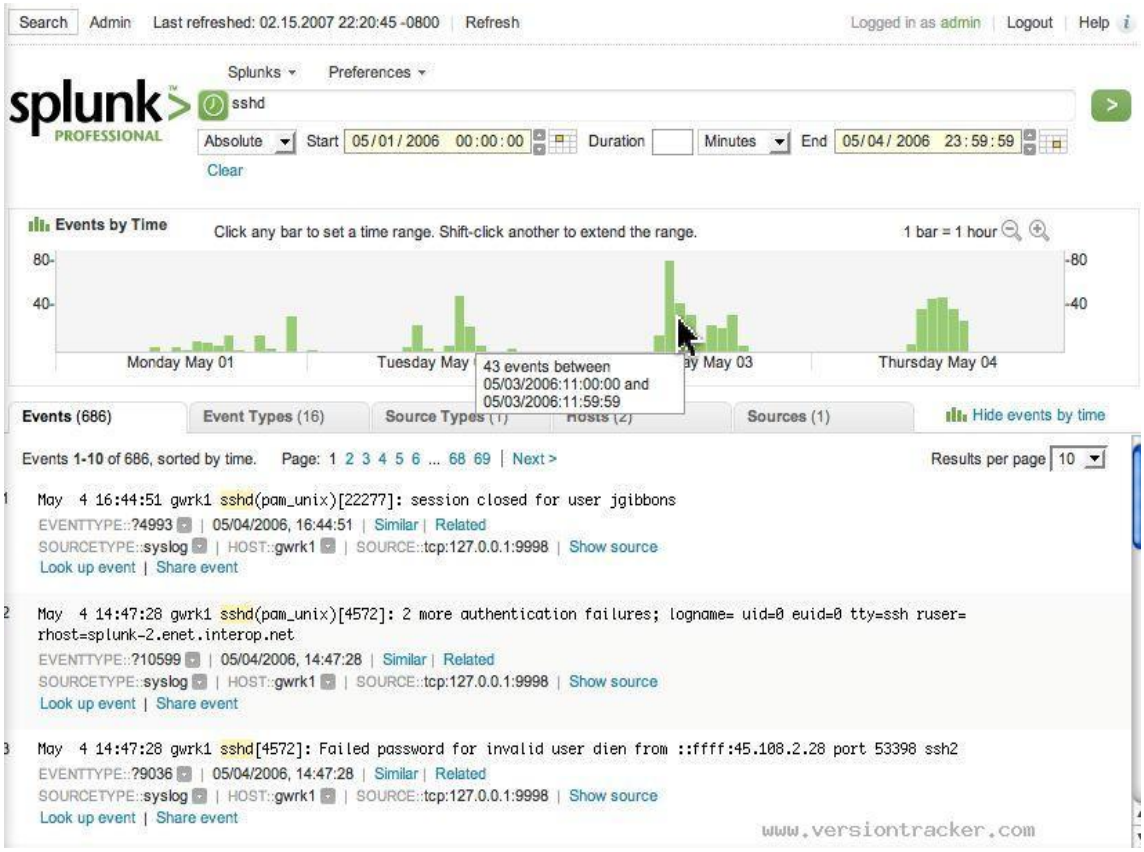

Figura 15. Interfaz Web del Servidor de Splunk.

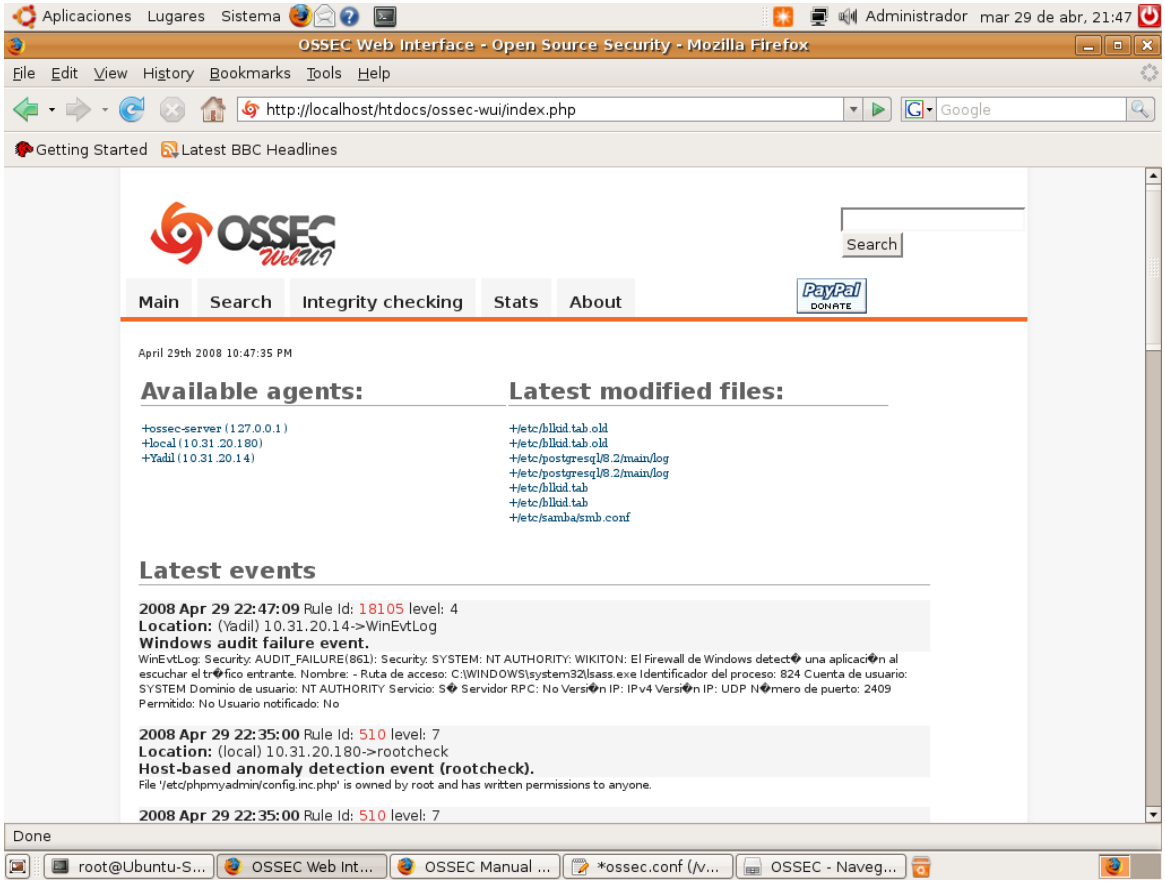

Figura 16. Interfaz Web del servidor de OSSEC.

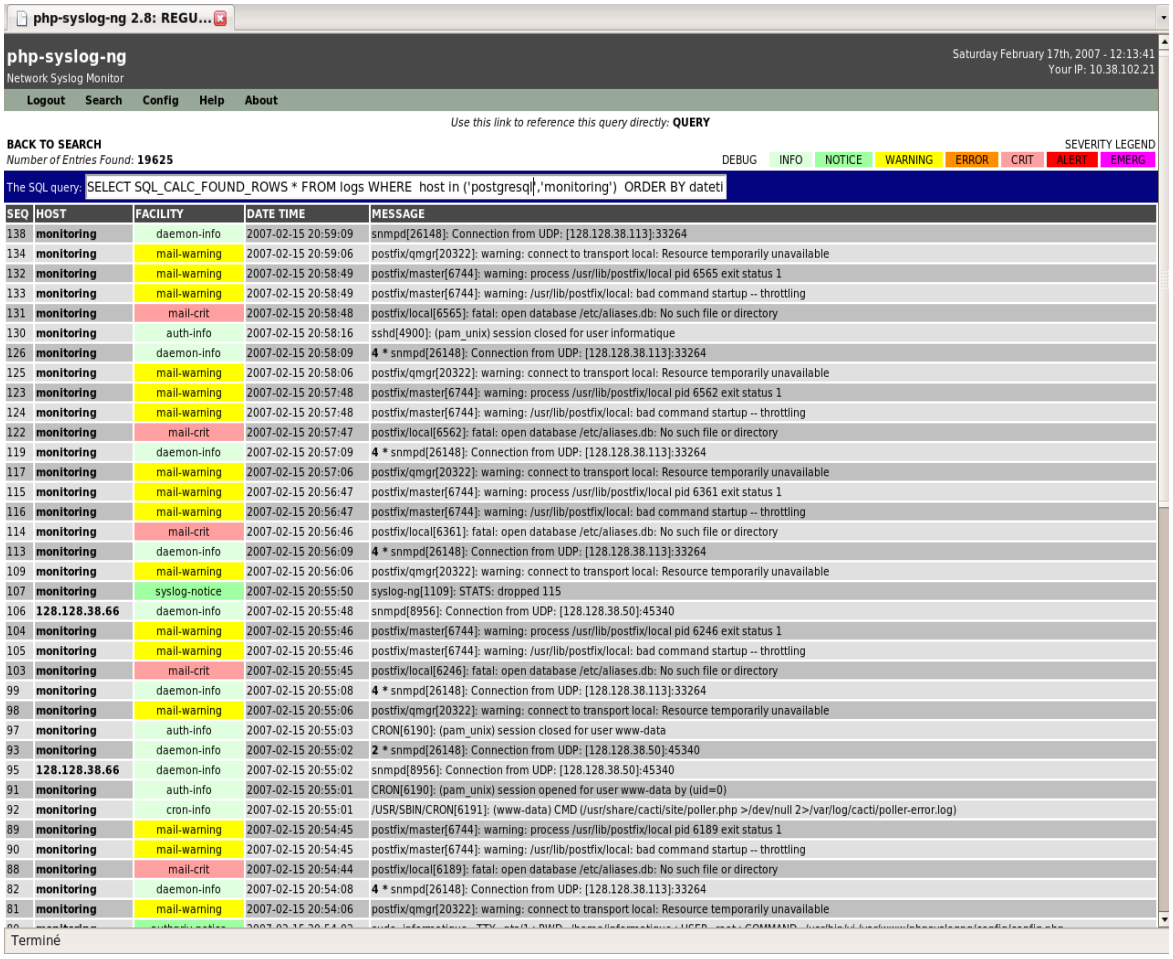

Figura 17. Interfaz Web Php-syslog-ng.

```
#------------------------
options
  {
    chain_hostnames(no);
    create_dirs (no);
    dir_perm(0755);
    dns_cache(yes);
    keep_hostname(yes);
    log_fifo_size(2048);
    log_msg_size(8192);
    long_hostnames(on);
    perm(0644);
    stats(3600);
    sync(0);
    time_reopen (10);
    use_dns(yes);
    use_fqdn(yes);
  };
```

Figura 18. Configuración del grupo “Option” del Syslog-ng como servidor.

```
#-------------------------------------------------------------------
source s_dgram
  { unix-stream("/dev/log"); };

source s_internal
  { internal(); };

source s_kernel
  { pipe("/proc/kmsg" log_prefix("kernel: ")); };

source s_tcp
  { tcp(ip(0.0.0.0) port(5800) keep-alive(yes) max_connections(1000)); };

source s_udp
  {udp(ip(0.0.0.0) port(6161)); };
```

Figura 19. Configuración del grupo “Source” de Syslog-ng como servidor.

```
#  Standard Log file locations
#-----------------------------------------------------------------------
destination authlog        { file("/var/log/auth.log"); };
destination bootlog        { file("/var/log/boot"); };
destination debug          { file("/var/log/debug"); };
destination explan         { file("/var/log/explanations"); };//No esta
destination messages       { file("/var/log/messages"); };
destination routers        { file("/var/log/routers.log"); };//No esta
destination secure         { file("/var/log/secure"); };
destination spooler        { file("/var/log/spooler"); };// No esta
destination syslog         { file("/var/log/syslog"); };
destination user           { file("/var/log/user.log"); };
#-----------------------------------------------------------------
#  Piping method
#-----------------------------------------------------------------
 destination database      {pipe("/tmp/mysql.pipe"
                           template("INSERT INTO logs (host, facility,
                           priority, level, tag, datetime, program,
                           msg) VALUES ( '$HOST', '$FACILITY', '$PRIORITY',
                           '$LEVEL', '$TAG', '$YEAR-$MONTH-$DAY-$HOUR:$MIN:$SEC', '$PROGRAM', '$MSG' );\n")
                           template-escape(yes)); };
```

Figura 20. Configuración del grupo “Destination” de Syslog-ng como servidor.

```
#-----------------------------------------------------------------------
filter      f_auth         { facility(auth, authpriv); };
filter      f_authpriv     { facility(authpriv); };
#filter      f_cron         { facility(cron); };
filter      f_daemon       { facility(daemon); };
filter      f_kern         { facility(kern); };
filter      f_local1       { facility(local1); };
filter      f_local2       { facility(local2); };
filter      f_local3       { facility(local3); };
filter      f_local4       { facility(local4); };
filter      f_local5       { facility(local5); };
filter      f_local6       { facility(local6); };
filter      f_local7       { facility(local7); };
filter      f_lpr          { facility(lpr); };
filter      f_mail         { facility(mail); };
filter      f_messages     { facility(daemon, kern, user); };
filter      f_news         { facility(news); };
filter      f_spooler      { facility(uucp,news) and level(crit); };
filter      f_syslog       { not facility(auth, authpriv) and not facility(mail); };
filter      f_user         { facility(user); };

#-----------------------------------------------------------------------
#  Other catch-all filters
#-----------------------------------------------------------------------
filter      f_crit         { level(crit); };
#filter     f_debug        { not facility(auth, authpriv, news, mail); };
filter      f_debug        { level(debug); };
filter      f_emergency    { level(emerg); };
filter      f_err          { level(err); };
filter      f_info         { level(info); };
filter      f_notice       { level(notice); };
filter      f_warn         { level(warn); };
```

Figura 21. Configuración del grupo “Filter” de Syslog-ng como servidor.

```
log { source(s_dgram);
      source(s_internal);
      source(s_udp);
      source(s_tcp);      filter(f_auth);      destination(authlog); };
log { source(s_dgram);
      source(s_internal);
      source(s_udp);
      source(s_tcp);      filter(f_local7);    destination(bootlog); };
log { source(s_dgram);
      source(s_internal);
      source(s_udp);
      source(s_tcp);      filter(f_local1);    destination(explan); };
log { source(s_dgram);
      source(s_internal);
      source(s_udp);
      source(s_tcp);      filter(f_local5);    destination(routers); };
log { source(s_dgram);
      source(s_internal);
      source(s_udp);
      source(s_tcp);      filter(f_messages);  destination(messages); };
log { source(s_dgram);
      source(s_internal);
      source(s_udp);
      source(s_tcp);      filter(f_authpriv);  destination(secure); };
log { source(s_dgram);
      source(s_internal);
      source(s_udp);
      source(s_tcp);      filter(f_spooler);   destination(spooler); };
log { source(s_dgram);
      source(s_internal);
      source(s_kernel);
      source(s_udp);
      source(s_tcp);      filter(f_syslog);    destination(syslog); };
```

Figura 22. Configuración del grupo “Log Path” de Syslog-ng como servidor.

```
options {
        check_hostname(yes);
        keep_hostname(yes);
        chain_hostnames(no);
        };
source inputs {
        internal();
        unix-stream("/dev/log");
                };
destination remote {
        udp("10.31.20.180" port(6161); );
                    };
log {
     source(inputs); destination(remote);
    };
```

Figura 23. Configuración Syslog-ng como agente.

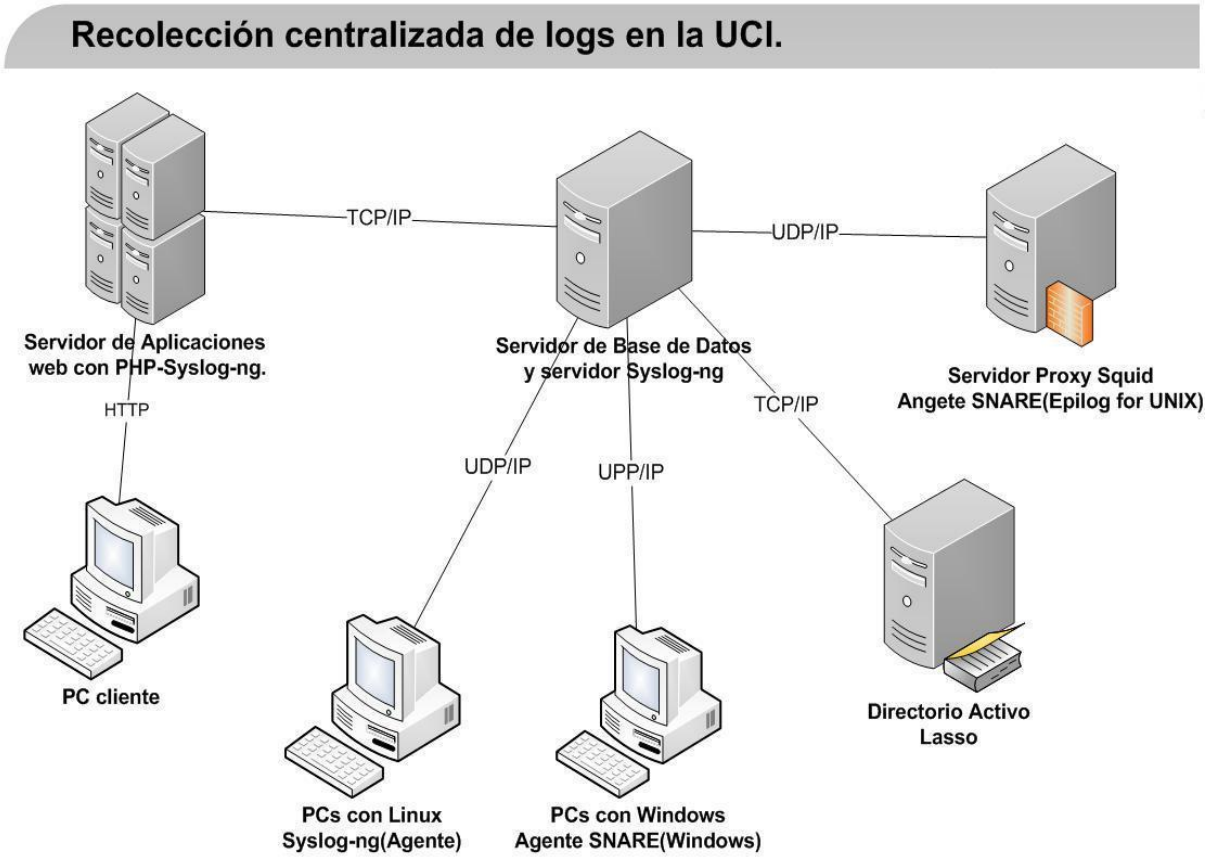

Figura 23. Arquitectura del sistema para la recolección de logs en la UCI.

GLOSARIO DE TÉRMINOS Y SIGLAS

AJAX: Es una técnica para el desarrollo de páginas Web.

Antivirus: Programas informáticos diseñados para detectar, bloquear así como eliminar otros programas y códigos malignos como pueden ser los virus, gusanos, etc.

Aplicación: Es un tipo de programa desarrollado con el objetivo de permitirle al usuario realizar determinados trabajos básicos para su trabajo en la PC como pude ser el procesamiento de texto, realizar cuentas, procesar imágenes, etc.

Archivo de Configuración: Este archivo contiene los parámetros de configuración a partir de los cuales funciona el programa.

Backup: copias de respaldo de determinados datos de tal forma que en caso de ocurrir algún incidente a los datos originales se pueda restablecer el sistema con la copia.

Barra de direcciones: Espacio donde se puede escribir y mostrar la dirección de una pagina web.

Base de Datos: Conjunto de datos relacionados y estructurados que son almacenados para un futuro uso.

Booleanas: Puede ser verdadero o falso.

Campos: Espacios que brindan las aplicaciones para que el usuario introduzca datos a esta.

Carpeta de Instalación: Contiene toda la implementación del software para ser instalado.

Cliente: En la informática es una aplicación que cuenta con las funcionalidades para acceder a determinados servicios que ofrece un servidor a través de la red.

Código abierto: El Software que brinda la posibilidad al usuario de acceder al código fuente.

Código fuente: Bloque de texto compuesto por líneas de códigos de un programa escritas según reglas de algún lenguaje de programación.

Controlador de Dominio: Servidor que se encarga de la seguridad de un dominio, administrando toda la información correspondiente a usuarios y recursos de su dominio. Todo dominio necesita un Controlador de Dominio.

Copia de respaldo: Realizar una copia de determinada información, así en caso de que los datos originales sean afectados se pueda restablecer el sistema con la copia antes hecha.

Criticidad: Nivel de importancia que se le da a un evento.

Cron: Programa usado en los sistemas operativos UNIX que puede ejecutar programas a intervalos de tiempo específicos.

Demonio: Es un tipo de proceso o programa informático no interactivo que se ejecuta en segundo plano en la computadora sin la intervención del usuario. Se ejecutan de forma continua sin parar. El término es usado en los sistemas operativos UNIX, al igual que en Windows se utiliza el término “servicio”.

Descomprimir: Con el objetivo de que los datos ocupen la menor cantidad de espacio posible son comprimidos. La descompresión es el proceso inverso en que los datos comprimidos son llevados a su estado normal.

Dirección IP: Es el acrónimo para Internet Protocol o Protocolo de Internet, son un número único e irrepetible con el cual se identifica una computadora conectada a una red.

Directorio Activo: Estructura de directorios utilizados en Microsoft Windows basado en computadoras y servidores para almacenar información y datos sobre redes y dominios.

Drivers: Programa que se encarga de manejar, gestionar y administrar determinadas acciones y recursos.

E-mail: El correo electrónico, en inglés “electronic email” o e-mail, es un método para crear, enviar y recibir mensajes a través de sistemas de comunicación electrónica.

Ética Informática: Disciplina que analiza problemas éticos que son creados por la tecnología de las computadoras o también los que son transformados o agravados por la misma, es decir, por las personas que utilizan los avances de las tecnologías de la información.

Fichero: Conjunto de datos, como pueden ser texto, gráficos, etc., que cuenta con una dirección específica en una computadora teniendo una identificación que es única formada por el nombre y la extensión. La extensión se refiere al tipo de datos que contiene.

Firewall: En español Cortafuego, es un sistema o conjunto de ellos ubicado entre dos redes o máquina y red que ejerce una política de seguridad establecida protegiendo una red confiable de una que no lo es.

GNOME: Entorno de escritorio creado para los sistemas operativos UNIX.

Grep: Herramienta que fue desarrollada originalmente para los sistemas operativos Unix, la cual toma una expresión regular, lee la entrada estándar o puede ser una lista de archivos para luego imprimir las líneas que contengan coincidencia para la expresión regular.

Host: En español anfitrión. Se refiere a una computadora conectada a la red que brinda o recibe servicios.

Indexar: Recoger y ordenar datos a partir de la utilización de índices.

IPv4 e IPv6: Internet Protocol versión 4 e Internet Protocol versión 6. Protocolos de Internet, la versión 4 se refiere a que las computadoras tienen direcciones IP de 4 números y las de versión 6 cuentan con direcciones de 6 números.

ISA: Servidor de Seguridad y Aceleración de Internet que controla el tráfico que pasa por las redes conectadas a este actuando como firewall.

Kernel: Termino informático en inglés que significa “núcleo”. Es el componente central de la mayoría de los sistemas operativos y tiene la responsabilidad de gestionar los recursos del sistema como la memoria, los dispositivos, los procesos, así como la comunicación entre el hardware y el software de la maquina.

Lanzó: En la informática el lanzamiento se refiere al hecho de publicar o sacar a la luz algo.

Lenguaje de programación: Permite la comunicación entre el programador y la máquina. Así el primero puede ordenar a la computadora a que realice todas las funciones necesarias.

Licencia libre: Permite las hacer uso de las libertades que brinda el software libre.

Licencia Pública de GNU: Garantiza la libertad de compartir y modificar software, para asegurar que el software es libre para todos sus usuarios.

Loguea: Llevar a cabo la acción de loguearse, que proviene del término informático inglés “login”, y que se puede traducir como “entrar en”. Es el proceso por el cual se le pide al usuario que se identifique con un nombre y una contraseña mediante la cual se comprueba si éste tiene derechos de acceso.

Mb: Mega Bytes. Unidad de medida utilizada en la informática.

Navegador web: En inglés “browser”, es un programa informático que permite visualizar y navegar por las páginas web entre otras cosas.

Not, Or, And: Operadores booleanos “No”, “O” e “Y”.

PIX (CISCO firewall): Una versión de firewall.

Plataformas: Un entorno sobre el que se ejecutan programas.

Políticas de seguridad: Conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica qué está y qué no está permitido en el área de seguridad.

PostgreSQL: Un gestor de base de datos.

Privilegios: Acciones que puede realizar un usuario en una computadora. Solamente el administrador cuenta con todos privilegios.

Procmail: Programa que permite procesar correos, de una forma sencilla pero muy potente.

Protocolo: En la informática es un conjunto especial de reglas y determinaciones que se utiliza en una conexión para efectuar una comunicación. Ambos lados deben reconocer y obedecer el protocolo para poder comunicarse.

Remota: Controlar o realizar determinadas acciones en una computadora desde otra.

Root: Es el nombre por defecto de la cuenta de usuario en los sistemas operativos Linux, que cuenta con todos los privilegios en la computadora. También es conocido como súperusuario y sin esta no se pueden realizar muchas tareas como instalar programas.

Rootkit: Software que se instala en una PC de forma oculta dejando una entrada secreta permitiendo la entrada de alguna persona sin el conocimiento del usuario.

Routers: En español enrutador o encaminador. Dispositivo de hardware que interconecta redes de computadoras asegurando el enrutamiento de los paquetes entre redes, además determina la ruta que debe tomar para llegar a su destino.

Script: Conjunto de instrucciones para la automatización de determinadas tareas.

Servicio: Término para referirse a los demonios en Windows.

Servidor: En la informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. Actualmente este término se utiliza también para referirse a la computadora o máquina en el cual funciona ese software que provee datos de modo que otras máquinas puedan utilizarlos e incluso almacenar otros.

Servidores DNS: Domain Name Server o Servidor de Nombres del Dominio. Se encarga de asignarle a cada computadora de su red un nombre en correspondencia con su IP.

Sesión: La conexión que establece el usuario con el sistema, mediante el inicio de sesión, utilizando los datos de acceso suministrados durante el registro. Así cuenta con un conjunto de programas, configuraciones y recursos. Puede iniciar una sesión posterior en el sistema con el mismo conjunto de programas en ejecución, configuraciones y recursos que los que disponía cuando finalizó la sesión anterior.

SMTP: Protocolo Simple de Transferencia de Correo. Protocolo utilizado para intercambiar mensajes a través del correo electrónico, para lo cual cuenta con un complejo servicio de correo a través de servidores.

Sniffer: Programa que se puede utilizar para capturar datos lícitamente o no que pasan por la red, de ahí que son muy usados para capturar contraseñas u otros datos confidenciales.

Software: Está formado por una serie de instrucciones y datos, que permiten aprovechar todos los recursos de la computadora.

Spool: Buffer de almacenamiento.

SSL, TSL: Protocolos para la encriptación de datos que viajan por la red.

Tiempo Real: Los sistemas de tiempo real son aquellos que tienen la capacidad de interactuar con su entorno físico de manera rápida, con respuestas dinámicas y conocidas en relación con los datos que reciben como entradas, salidas y restricciones temporales.

Webcaché: Servidores que los proveedores de internet utilizan para almacenar páginas web. Así, cuando sus clientes quieren ver una web la mandan desde el Webcaché agilizando la conexión.