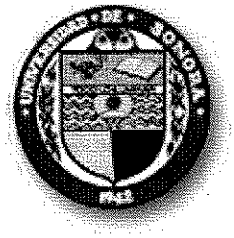
UNIVERSIDAD DE SONORA

DIVISIÓN DE INGENIERIA

INGENIERÍA EN SISTEMAS DE INFORMACIÓN



ESTANCIAS PROFESIONALES

"MONITOREO DE LA RED CAMPUS HERMOSILLO DE LA UNISON"

ELABORADO POR:

JESUS ALAN VILLEGAS CADENA

ASESOR EXTERNO:

ARNOLDO F. VIDAL ROMERO

HERMOSILLO, SONORA A SEPTIEMBRE DEL 2009

ÍNDICE

Introducción 1

Justificación 2

Objetivos 4

Características del área en que se participó 6

Problemas a resolver 9

Alcances y Limitaciones 11

Fundamento Teórico 13

Procedimiento y Descripción de las Actividades Realizadas. 20

Parte 1.- Instalación de un nuevo nodo 21

1.1.- Configuración de Hardware 21

1.2.- Configuración del Sistema Operativo 21

1.3.- Instalación de PCRE y Snort 22

1.4.- Configuración de Snort 23

1.5.- Actualización del Servidor 26

Parte 2.- Instalación y Configuración de BASE 29

2.1.- Uso y Configuración de BASE 30

2.2.- Reportes Predeterminados 32

2.3.- Búsqueda 37

2.4.- Graph Alert Data 40

2.5.- Menús de Administración 42

Resultados, Planos, Gráficas, Prototipos y Programas 52

Fortalezas y Debilidades 56

Oportunidades y Recomendaciones. 57

Conclusiones y Recomendaciones 59

Referencias Bibliográficas y Virtuales 61

Introducción

La seguridad en las redes y telecomunicaciones en la actualidad es bien difícil de establecer y adquirir, ya que siempre los accesos no autorizados se hacen presentes para adquirir información y datos confidenciales, el cual dicha información puede afectar a la organización que la posee. Es por eso que es primordial conocer y aplicar las herramientas de monitoreo de trafico de red para poder salvaguardar la información de la empresa o en este caso la institución educativa.

Por medio de este documento se presenta la realización del proyecto monitoreo de redes en la Universidad de Sonora, en el cual se describirá el proceso completo que se tuvo que llevar para su implementación dentro del campus, así como también la experiencia adquirida a través de este proyecto, la problemática que se resolvió y el status del proyecto en el campus. Se explicará de manera detallada de que manera se implementó el monitoreo de redes para incrementar la seguridad en la universidad y que resultados produjo una vez puesto en marcha el proyecto dentro del campus universitario.

El desarrollo del proyecto depende de las configuraciones hechas a los servidores y equipos de cómputo que se utilizaron para la implementación de los nodos en distintas sectores de nuestra alma Mater, para monitorear el tráfico de red en los distintos departamentos que componen a la Universidad, en el cual dicho proceso esta descrito en este documento.

Justificación

Este proyecto se hace con el propósito de mejorar la seguridad de la red campus Hermosillo de la Universidad de Sonora. La seguridad en las redes de la universidad de Sonora es prioritario ya que la información que se maneja dentro del campus es muy importante, tales como calificaciones de los alumnos, registros bancarios, datos presupuestos y dinero a invertir en proyectos, todos en los cuales tienen cierto nivel de confidencialidad ya que no cualquier persona tiene acceso a verlos o alterarlos de cualquier modo.

Por eso es importante aplicar reglas y medidas de seguridad para asegurar los datos e información confidenciales para la institución, en cual dicho caso aplicaremos el proyecto Snort para monitorear el tráfico en la red con el objetivo de detectar cualquier anomalía, accesos no autorizados o traslado de información que no se debe mover o modificar.

Es necesario procurar limitar el acceso a las redes mediante niveles jerárquicos dentro de la institución por medio de cuentas de usuario que permitan las distinciones de esos niveles para poder desplegar la información adecuada y a la cual tienes acceso el usuario al momento de ingresar. No obstante, es necesario llevar un control de las actividades que se realizan diariamente así como también los accesos que se hacen a los sistemas en los distintos niveles jerárquicos de la institución. Es por eso que se instalarán nodos en cada uno de los departamentos del campus para tener mayor control sobre el tráfico de la red.

Una fuente de información importante para la Escuela es la Intranet, la cual almacena mucha información confidencial o restringida a grupos de usuarios específicos, por esta razón es manejada con un nivel de seguridad alto. Los computadores personales de usuarios de la Escuela muchas veces mantienen información importante y confidencial, por lo tanto se deberían proteger casi de la misma forma que la Intranet.

Objetivos

- ✓ Diseñar un sistema de monitoreo que permita detectar oportunamente posibles ataques a la red de datos de la Universidad de Sonora campus Hermosillo.

Con esto se quiere llegar con el proyecto para brindar mayor seguridad tanto para los equipos como a las personas en la institución contra los que buscan acceder a información que es exclusiva para la empresa y buscan de algún modo hacer daño a dicha institución robando la información y usándola para su beneficio.

- ✓ Detener e identificar las anomalías o ataques detectados una vez implementado el proyecto de monitoreo de trafico de red.

Es necesario saber las fuentes por las cuales se causan las amenazas de ser atacado por un intruso para eliminar las posibilidades de ser atacado por la misma fuente y así poder lograr detener los ataques a la red de datos y proporcionar un nivel de seguridad alto y confiable.

- ✓ Proporcionar protección a la red de datos cuidando el tráfico que se genera dentro del campus universitario.

El resguardo de la información en la red es muy importante, más si se trata de una institución educativa en donde se lleva una gran cantidad de información sobre las calificaciones de los alumnos, del departamento de tesorería e información de proyectos presupuestales en los que la institución ha invertido una seria cantidad de dinero, entre otros. El manejo de ese tipo de información conlleva una gran responsabilidad para la institución, ya que las violaciones de acceso de red siempre están presentes para lograr

robar ese tipo de información, causando así daños no solo a la institución, sino a los alumnos, maestros, etc.

Así mismo al cuidar el trafico de red, cuidamos el equipamiento de red, los servidores, el ancho de banda, etc. son recursos que las organizaciones también deben cuidar y proteger, ya que en ellos se levanta la plataforma informática utilizada a diario. Estos recursos además de ser costosos, son una parte medular de toda organización.

Características del área en que se participó

El proyecto se desarrolló en el área de redes en la Dirección de Informática de la Universidad de Sonora, con el cual dicho proyecto conlleva de los recursos de esa área para poder llevarlo acabo. El área de redes, es el encargado de proporcionar el servicio de Internet, así como el arreglo y monitoreo de las redes tanto alambicas como inalámbricas dentro del alma mater. Proporciona el mantenimiento y soporte técnico necesario a todo el equipo de redes tales como Aps(Access points), switches, routers, configuraciones a los servidores y equipos de red.

El proyecto va enfocado en la ayuda de la restauración de monitoreo de privilegios de acceso y movimientos en la red de datos como también proporcionar y asegurar la confianza y seguridad de los datos en los distintos lugares de la unison. Este proceso forma parte íntegra del área de redes ya que es una de las principales funciones que desarrolla dentro de la universidad.

Este proyecto esta dedicado hacia la parte de redes ya que se enfoca totalmente a monitorear constantemente el tráfico de red de datos y verificar el traspaso de información de los equipos en el campus así como también detectar cualquier anomalía existente para la información que trafica la red en si.

Se escogió ésta área para expandir los conocimientos en redes y comunicaciones para poder competir con el mercado laboral de hoy en día y así poder lograr una mayor oportunidad de empleo.

En el área de redes existe:

1 Encargado de configuración de las redes inalámbricas

1 Encargado de la seguridad y detección de intrusos

1 Encargado de cableado estructurado y configuración de aps

1 Jefe de área de redes

El encargado de las redes inalámbricas mantiene y se encarga del correcto funcionamiento y establecimiento de la señal de las redes inalámbricas en el campus, así como las configuraciones de los puntos de acceso en las distintas localizaciones de la universidad.

El encargado de seguridad atiende las inquietudes de establecimiento de normas de seguridad de red, que permitan la interacción de los dato en una red segura y libre de intrusos. Es por ende que las nuevas tecnologías exigen calidad y prestigio en lo que respecta a los nuevos inquilinos de la red.

El encargado de cableado estructurado, revisa la configuración de los switches y los routers en los que están conectados los aps, y además da prioridad a los procedimientos que se deben de seguir para la colocación estratégica de los puntos de acceso y de la propagación homogénea de la señal en los edificios del campus Hermosillo.

El jefe del área, que en este caso es el área de redes de la dirección de Informática, establece las estrategias a seguir y los lineamientos que se tienen que seguir

para asegurar el funcionamiento correcto de la estructura de la red de datos en la universidad.

Problemas a Resolver

Caso 1: diferentes estudios nos demuestran que la mayoría de los ataques realizados en una red hacia sus servidores de misión crítica son efectuados desde dentro de las organizaciones. Nuestro caso no puede estar ajeno a estas estadísticas debido a la naturaleza de la información y la importancia de la misma hacia la comunidad, aumentándose este riesgo debido a la facilidad que tiene la red de conectar equipos en ellas. Si la mayoría de las veces no es la intención el mal uso de los recursos, ni vulnerar sistemas, la falta de políticas de seguridad genera e incrementa estos problemas. Por ejemplo, podría presentarse el caso de que alguien en la institución conecte su computadora personal a la red, tomando una IP sin solicitar, en el caso de que esta computadora llegara a estar infectada, este virus se propagaría primero por la subred donde se instalo y después al resto de las redes, hasta donde sea permitido su tráfico, causando un consumo exagerado de los recursos de la red.

Caso 2: Otro problema que se puede presentar está relacionado con los servidores de los departamentos o de proyectos, que no cuentan con un ningún nivel de seguridad aceptable. Estos equipos pueden ser vulnerados (hackeados) y utilizados para propósitos ajenos al quehacer de los mismos departamentos generando *denegaciones de servicio distribuidas*. Este tipo de ataques tienen como objetivo provocar la caída de un servicio, mediante la saturación del servidor con peticiones realizadas desde muchos computadores a la vez.

Caso 3: El uso de las computadoras como servidores dedicados a juegos, que pueden comprometer los enlaces de los departamentos o de la misma red. Esto trae

como consecuencia de que las personas conectadas a servidores dentro de la unison de manera externa, puedan obtener acceso a información al hacerse pasar por otro jugador más en los juegos de los servidores.

Caso 4: Un intento claro de mal uso de la red, aquí es difícil detectar y encontrar a los responsables, a menos que se cuente con las herramientas de control y sobre todo, de las políticas que respalden las acciones a ejercer sobre los responsables de los daños a la red.

En casi todos los casos puede detectarse un uso excesivo en la red. Esto podemos minimizarlo utilizando controles y políticas mas restrictivas, pero que nos conducen a otro tipo de problemática social o política por parte de los usuarios, por lo que debemos mantener un programa constante de monitoreo o vigilancia que nos permita detectar a tiempo un caso de los mencionados anteriormente.

En los nodos principales de la red, pretendemos instalar un equipo configurado con LINUX y ejecutando software libre (SNORT). Este equipo mediante el programa mencionado, permite capturar tráfico de manera promiscua, sin interferir de manera considerable en el trafico de la red, y permitiendo obtener información mediante comparación con patrones definidos de ataques para poder distinguirlos y proceder a un análisis mas detallado, utilizando otros programas comerciales adquiridos para estos fines.

Alcances y Limitaciones

Los alcances de este proyecto fueron los siguientes:

- Se realizó la configuración e instalación del software en los nodos de monitoreo, así como la modificación de reglas de snort para el buen funcionamiento del nodo.

- La instalación de un servidor central, el cual permite el control de la base de datos que por medio de ella se guarda la información de los paquetes monitoreados de los 6 nodos que están monitoreando la red.

- Se realizó documentación del proyecto, para el manejo futuro de los nodos y creación del servidor central, así como la especificación de las configuraciones necesarias para poder realizarlo.

- La implementación y terminado de lo 6 nodos de monitoreo en diferentes departamentos de la universidad de sonora, en los cuales es donde son áreas de trafico pesado en la red.

- El mantenimiento oportuno de los nodos, así como el mantenimiento de la base de datos del servidor central.

Limitaciones

La confidencialidad de la empresa no dejo la manipulación eficiente de la información, debido al acceso limitado que se tuvo en el monitoreo de la red.

Debido a que los nodos y el servidor eran computadoras recicladas y de bajo rendimiento, la información que se recolectaba era limitada ya que se tenía que limpiar la base de datos cada semana.

Fundamento Teórico

SNORT es un software libre para detección de intrusos y capaz de generar un sistema de prevención mediante el análisis de paquetes en tiempo real del tráfico de las direcciones IP de la red. SNORT fue escrito por Martin Roesch pero actualmente es de Sourcefire, de la cual Roesch es fundador y actualmente su director principal.

SNORT puede desempeñar un análisis de protocolo, búsqueda y comparación de contenidos y puede ser usado para detectar varios tipos de ataques y pruebas, como buffer overflows, robos, escaneo de puertos, ataques en aplicaciones web, y otros más. Puede ser utilizado con propósitos de prevención de intrusos, por tomar muestras de ataques en el mismo lugar donde se ejecutan. Combinado con otros programas como SNORTSNARF, SGUIL, OSSIM y BASE puede proveer una representación visual de la información obtenida de la intrusión. Con las debidas actualizaciones, puede ser soporte para ataques por flujo de virus y anormalidades de la red en capas 3 y 4, mediante observación histórica.

En 1998, Martin Roesch escribió una tecnología de software libre llamado Snort, el cual el lo señalaba con el termino "versión ligera" a la tecnología de detección de intrusos en comparación a los sistemas comerciales disponibles. Hoy en día, ese termino ni siquiera comienza ha describir las capacidades que Snort brinda. A través de los años, Snort ha evolucionado en una tecnología madura, llena de características, el cual se ha convertido en el standard de detección y prevención de intrusos. Avances recientes tanto en reglas en el lenguaje como en las capacidades de detección, ofrecen

las mas flexible y eficaz detección de amenazas disponible, haciendo a Snort el campeón de pesos pesados en prevención de intrusos.

BASE sus siglas en ingles que significa Basic Analysis and Security Engine (Motor básico de búsqueda y seguridad). Esta basado en el código de ACID (Analysis Console for Intrusion Databases) Consola de Análisis para Base de Datos de Intrusos. Esta aplicación proporciona consultas de bases de datos con interfaz de php en el navegador para mostrar grafica y visualmente la información que SNORT detecta en la red que esta siendo monitoreada.

BASE es una interfaz en web para desarrollar análisis de accesos no autorizados que snort ha detectado en la red. Base se le da soporte por un grupo de voluntarios que colaboran día con día en el proyecto de base.

BarnYard es un sistema de salida de Snort. Snort crea un archivo especial de binario llamado "unified". Barnyard lee este archivo, y luego lo reenvía los datos a la base de datos de Snort. Barnyard detecta los errores de envío de alertas a la base de datos cuando se presentan, por lo cual deja de mandar alertas. También detecta cuando la base de datos puede aceptar conexiones de nuevo y así empezar a mandar alertas otra vez, esa es básicamente la función de barnyard con snort.

Software Libre es la denominación del software que brinda libertad a los usuarios sobre su producto adquirido y por tanto, una vez obtenido, puede ser usado, copiado, estudiado, modificado y redistribuido libremente. Según la *Free Software Foundation*, el software libre se refiere a la libertad de los usuarios para ejecutar, copiar,

distribuir, estudiar, cambiar y mejorar el software; de modo más preciso, se refiere a cuatro libertades de los usuarios del software: la libertad de usar el programa, con cualquier propósito; de estudiar el funcionamiento del programa, y adaptarlo a las necesidades; de distribuir copias, con lo que puede ayudar a otros; de mejorar el programa y hacer públicas las mejoras, de modo que toda la comunidad se beneficie (para la segunda y última libertad mencionadas, el acceso al código fuente es un requisito previo).

El software libre suele estar disponible gratuitamente, o al precio de coste de la distribución a través de otros medios; sin embargo no es obligatorio que sea así, por ende no hay que asociar software libre a "software gratuito" (denominado usualmente freeware), ya que, conservando su carácter de libre, puede ser distribuido comercialmente ("software comercial"). Análogamente, el "software gratis" o "gratuito" incluye en algunas ocasiones el código fuente; no obstante, este tipo de software *no es libre* en el mismo sentido que el software libre, a menos que se garanticen los derechos de modificación y redistribución de dichas versiones modificadas del programa.

Tampoco debe confundirse software libre con "software de dominio público". Éste último es aquél que no requiere de licencia, pues sus derechos de explotación son para toda la humanidad, porque pertenece a todos por igual. Cualquiera puede hacer uso de él, siempre con fines legales y consignando su autoría original. Este software sería aquél cuyo autor lo dona a la humanidad o cuyos derechos de autor han expirado, tras un plazo contado desde la muerte de éste, habitualmente 70 años. Si un autor condiciona su uso bajo una licencia, por muy débil que sea, ya no es dominio público.

Sistema Operativo se encarga de crear el vínculo entre los recursos materiales, el usuario y las aplicaciones (procesador de texto, videojuegos, etcétera). Cuando un programa desea acceder a un recurso material, no necesita enviar información específica a los dispositivos periféricos; simplemente envía la información al sistema operativo, el cual la transmite a los periféricos correspondientes a través de su driver (controlador). Si no existe ningún driver, cada programa debe reconocer y tener presente la comunicación con cada tipo de periférico. De esta forma, el sistema operativo permite la "disociación" de programas y hardware, principalmente para simplificar la gestión de recursos y proporcionar una interfaz de usuario sencilla con el fin de reducir la complejidad del equipo.

Fedora Core es una distribución de GNU/Linux para propósitos generales basada en RPM , que se mantiene gracias a una comunidad internacional de ingenieros, diseñadores gráficos y usuarios que informan de fallos y prueban nuevas tecnologías. Cuenta con el respaldo y la promoción de Red Hat.

El proyecto no busca sólo incluir software libre y de código abierto, sino ser el líder en ese ámbito tecnológico. Algo que hay que destacar es que los desarrolladores de Fedora prefieren hacer cambios en las fuentes originales en lugar de aplicar los parches específicos en su distribución, de esta forma se asegura que las actualizaciones estén disponibles para todas las variantes de GNU/Linux.[2] Max Spevack en una entrevista afirmó que: "Hablar de Fedora es hablar del rápido progreso del Software Libre y de Código Abierto".Durante sus primeras 6 versiones se llamó *Fedora Core*, debido a que solo incluía los paquetes más importantes del sistema operativo.

Servidores

Como su nombre lo indica, son los dispositivos de red que brindan un servicio a otros dispositivos (clientes). En general quien realiza esta tarea es un software especializado, pero comúnmente se conoce como servidor al equipo físico donde se ejecuta, el cual es el centro de la infraestructura de la red. En redes pequeñas es común que un equipo brinde varios servicios simultáneamente como, por ejemplo, un servidor de archivos el cual también es servidor de impresión. Partiendo de esta definición, cualquier computadora en la red puede ser un servidor sin necesidad de contar con un hardware o software en particular; aunque existen sistemas operativos especializados (como Microsoft Windows Server, Debian GNU/Linux y SUN Solaris entre otros) los cuales fueron diseñados específicamente para optimizar los recursos que se comparten a la red. De la misma manera, existen equipos puntualmente creados para funcionar con grandes volúmenes de información, durante las 24hs y con mejor rendimiento y velocidad que el hardware de escritorio

Servidor de base de datos Proporciona servicios de acceso, gestión, administración y protección a una o varias bases de datos a través de la red. Dichos servidores solucionan los problemas de las empresas al manejar grandes volúmenes de información de una manera estable, fiable, coherente y segura en un entorno heterogéneo de trabajo y de necesidades de información .La mayoría de los motores de bases de datos cuentan con mecanismos que permiten el acceso remoto a la misma, pudiendo entonces transformar al equipo que contiene la base de datos en un servidor.

Router/Switch

El Router es, como la palabra lo dice, un rutador/encaminador. Es un dispositivo para la interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. El router interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red. El router toma decisiones (basado en diversos parámetros) con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados.

El Switch. Es un dispositivo de red que filtra, envía e inunda de frames en base a la dirección de destino de cada frame. Opera en la capa dos (nivel de red) del modelo OSI. Término general que se aplica a un dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.

Base de Datos

Una base de datos es un "almacén" que nos permite guardar grandes cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente.

El término de bases de datos fue escuchado por primera vez en 1963, en un simposio celebrado en California, Estados Unidos. Una base de datos se puede definir como un conjunto de información relacionada que se encuentra agrupada o estructurada.

Desde el punto de vista informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulen ese conjunto de datos.

Cada base de datos se compone de una o más tablas que guarda un conjunto de datos. Cada tabla tiene una o más columnas y filas. Las columnas guardan una parte de la información sobre cada elemento que queramos guardar en la tabla, cada fila de la tabla en la cual se conforma cada uno de los registros en la base de datos.

Procedimiento y Descripción de las Actividades Realizadas

Introducción

En la actualidad existe una gran preocupación por la seguridad de los datos que se transmiten en una red de computadoras. Nunca se puede estar 100% seguro de que lo que hagamos sea completamente confidencial ni de que todos los usuarios de una red tengan intenciones legítimas.

Es por esto que se han desarrollado soluciones de software con la finalidad de monitorear la actividad que pasa en una red, para que los administradores tengan una idea de qué es lo que pasa dentro de ella. Una de estas soluciones es el sistema Snort, una herramienta de uso libre que analiza el tráfico de una red basándose en una serie de patrones de comportamiento y tráfico común cuando existen actividades maliciosas o sospechosas. Para la mejor interpretación de estos resultados se utilizó el Motor Básico de Análisis y Seguridad (BASE, por sus siglas en inglés) el cual genera reportes y búsquedas de los datos guardados por Snort.

El presente manual describe cómo añadir nodos sensores en la red de monitoreo previamente instalada en el Campus Hermosillo de la Universidad de Sonora y la forma de utilizar la interfaz web de BASE. Se espera que el lector tenga conocimientos previos básicos de redes de computadoras, el manejador de bases de datos MySQL y el sistema operativo Fedora.

1. Instalación de un nuevo nodo

El proyecto fue desarrollado pensando en utilizar equipos "de reciclaje" como nodos sensores, por lo cual no es necesario emplear equipo de última generación. De los nodos instalados, el equipo con menos recursos cuenta con procesador Pentium 2 a 400 MHz. En caso de que equipos similares se utilicen, se debe compensar la falta de capacidad de procesamiento con memoria RAM de por lo menos 256 MB, como es el caso del equipo antes mencionado.

1.1 Configuración de Hardware

Los requerimientos de hardware para un nuevo nodo sensor son:

- Compatible con Fedora Core 3.
- 2 Interfaces Ethernet.

Es importante considerar que una de las dos interfaces de red del equipo debe estar conectada a un puerto mirror o similar del equipo de red. Esta interfaz debe ser la interfaz denominada eth1 por el sistema operativo, mientras que la interfaz denominada eth0 debe estar conectada a un puerto normal del equipo de red para poder tener salida a la misma.

1.2 Configuración de Sistema Operativo

Se recomienda fuertemente instalar el sistema operativo Fedora Core 3, para evitar posibles incompatibilidades con otras versiones. Durante la instalación se debe

introducir la dirección IP para cada una de las interfaces de red y seleccionar la opción "Habilitar al Inicio". Para evitar que el equipo baje su rendimiento, se debe instalar con el menor número de paquetería, pero cuidando que las siguientes estén instaladas:

- Cliente MySQL.
- Servidor MySQL (necesario para la configuración de Snort).
- Las opciones por default al seleccionar "Herramientas de configuración del Servidor".
- Las herramientas de desarrollo incluidas por default, además de:
    - Expect.
    - Gcc-objc.
- Herramientas de Administración.
- Herramientas del Sistema.

1.3 Instalación de PCRE y Snort

Hacer lo siguiente como root. Una vez finalizada la instalación, se descargan tres archivos: el instalador de Snort y el instalador de PCRE (Perl Compatible Regular Expressions) desde sus respectivas páginas: http://www.snort.org/dl/ y http://umn.dl.sourceforge.net/sourceforge/pcre/ , respectivamente. También es necesario copiar el archivo conf.tar.gz que se encuentra en el servidor central.

Desde el directorio donde está el archivo que contiene los archivos comprimidos de los instaladores, se ejecuta el siguiente comando para ambos instaladores (Snort y PCRE):

tar –xf **<nombre de archivo>**

* Si el comando falla, cambiar –xf por –zxf. Si ambos fallan, volver a descargar el archivo.

Con esto se descomprimen los instaladores de los programas y se crea un directorio por cada archivo, el cual contiene lo necesario para la instalación de los programas El primero que se debe instalar es PCRE ejecutando los siguientes comandos en orden:

```
./configure
make
make install
```

Al finalizar la instalación de PCRE, se procede a instalar Snort desde el directorio donde se descomprimió su instalador con los comandos:

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

1.4 Configuración de Snort

Para configurar snort se debe descargar al nodo el archivo conf.tar.gz desde el servidor central y descomprimir con el comando antes mencionado. Dentro del archivo

comprimido se encuentran los directorios etc y rules; estos directorios se deben mover al directorio /root. Una vez hecho el cambio de ruta, se debe acceder al archivo /root/etc/snort.conf y buscar la línea:

```
var HOME_NET any
```

Esta variable guarda las direcciones locales que se han de monitorear. Por ejemplo, suponiendo que el sensor monitoreará las redes 192.168.0.0 y 192.168.1.0, esta línea deberá escribirse como:

```
var HOME_NET [192.168.0.0/24,192.168.1.0/24]
```

Se pueden agregar tantas redes separadas por comas como sea necesario. También se pueden agregar hosts en específico, usando máscara de 32 bits. Es indispensable asegurarse que no existan espacios dentro de la lista.

También es necesario modificar la línea donde se guarda la red externa. Ésta línea está escrita como:

```
var EXTERNAL_NET any
```

Se debe cambiar a:

```
var EXTERNAL_NET !$HOME_NET
```

En la sección de bases de datos del mismo archivo, se debe buscar la línea:

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

para descomentarse y hacer los siguientes cambios:

output database: log, mysql, user=**<usuario nuevo>** password=**<password del usuario>** dbname=snort host=central

Con esta línea se habilita el registro de las alertas generadas en la base de datos que ya está creada en el servidor central. Es muy importante recordar el usuario nuevo y su password para poder darlo de alta en el servidor. Los accesos a la base de datos se configurarán más adelante.

Dentro del mismo archivo snort.conf, se puede configurar los tipos de reglas a analizar escribiendo un carácter '#' para que cierto tipo de reglas no se usen. Se recomienda no modificar la configuración inicial de estas reglas. Para añadir reglas existe el archivo local.rules, dentro del cual se pueden implementar reglas propias. Para ignorar todo el tráfico icmp de cierto equipo conectado a la red (por ejemplo un monitor de estado de conectividad) podemos añadir la siguiente regla en el archivo local.rules:

```
pass icmp 192.168.1.1 any <> any any
```

Dicha línea indica que se ha de dejar pasar sin crear una alerta todo el tráfico de protocolo icmp que tenga como fuente el host 192.168.1.1 en cualquier puerto (indicado

por el primer any) hacia cualquier dirección IP (segundo any) en cualquier puerto (tercer any) o en sentido contrario (indicado por <>). El parámetro icmp también se puede cambiar por tcp, udp o ip.

Para conocer más sobre el tema de creación de reglas con Snort, consultar http://www.snort.org/docs/snort_htmanuals/htmanual_2.4/node14.html .

En el archivo /etc/hosts se debe agregar la dirección del servidor central, en este caso se debe agregar la siguiente línea:

148.225.232.162 central

Por último, hay que configurar el nodo para iniciar en modo consola. Para esto se modifica el archivo /etc/inittab en la primera línea no comentada, y se modifica a:

id:3:initdefault:

Una vez terminada la configuración del nodo sensor, lo más recomendable es activar la opción de encendido automático en el BIOS y desactivar el fallo cuando no se encuentra teclado, para así poder remover pantalla, teclado y mouse para dificultar el acceso al sensor de personas no autorizadas.

1.5 Actualización del servidor

El siguiente paso es la configuración del servidor. Primeramente, se debe modificar el archivo /etc/hosts para registrar el nuevo nodo. Se debe seguir la

estructura de nominación y orden numérico de los hosts que ya están registrados en el archivo, para asegurar el buen funcionamiento de los scripts de monitoreo y activación de los sensores. Esto quiere decir que el nuevo nodo se debe registrar como:

xxx.xxx.xxx.xxx nodo**#**

Donde **xxx.xxx.xxx.xxx** es la dirección IP del nuevo nodo y **#** es el siguiente número en la lista.

Una vez está dado de alta el nuevo nodo en el archivo hosts, se debe modificar el archivo /usr/bin/initnodos para poder habilitar el inicio automático de Snort en el nodo. Para esto, agregamos el número de nodo en la primera línea.

A continuación, se debe transferir el archivo /root/.ssh/id_dsa.pub al nuevo nodo dentro de la carpeta /root/.ssh (en caso de que el directorio no exista, se debe crear). Esto se puede lograr con el comando scp. Una vez copiado el archivo se debe renombrar a authorized_keys2. Con esto seremos capaces de transmitir comandos directamente al nodo sin necesidad de introducir contraseñas.

Después es necesario configurar MySQL para permitirle al nodo acceder a la base de datos. Esto se puede hacer desde la consola de MySQL. Una vez en la consola, ejecutamos el comando:

mysql> grant all on snort.* to **<usuario>@<host>** identified by '**<password>**';

En **<usuario>** y **<password>** deben asignarse el nombre de usuario y contraseña escritos en el archivo snort.conf del sensor (solamente el password necesita comillas sencillas), mientras que en **<host>** debe introducirse el nombre de host añadido al archivo /etc/hosts del servidor central.

Una vez terminados estos pasos, se puede ejecutar el script:

/usr/bin/initnodes

El cual consulta el estado de todos los nodos y activa Snort en cualquier sensor dado de alta que no lo esté corriendo al momento de ejecutarse el script.

2. Instalación y Configuración de BASE

BASE, que en sus siglas en inglés significa Basic Analysis and Security Engine, provee un análisis detallado a través de una interfaz web de las alertas que el programa Snort detecta en el tráfico de la red para poder llevar a cabo un análisis detallado sobre las mismas y facilitarle al administrador seleccionar las acciones correctivas a aplicar. Esta aplicación solamente es necesaria en el servidor central, no en los nodos.

Antes de instalar el programa BASE se necesita tener instalados los programas que a continuación se mencionan:

- JPGraph (http://www.aditus.nu/jpgraph/downloads/jpgraph-1.16.tar.gz)
- ADODB (http://umn.dl.sourceforge.net/sourceforge/adodb/adodb460.tgz)
- BASE (http://umn.dl.sourceforge.net/sourceforge/secureideas/base-1.0.1.tar.gz)

Para la instalación del programa JPGraph se requiere primero bajarlo desde la dirección de Internet que se muestra arriba para después instalarlo como se indica a continuación.

```
cp jpgraph-1.16.tar.gz /var/www/html
cd /var/www/html
tar –xvzf jpgraph-1.16.tar.gz
rm –rf jpgraph-1.16.tar.gz
```

Con esto se copia el instalador al directorio /var/www/html, después accede a dicha carpeta y se descomprime el archivo dejando así una carpeta la cual nos servirá para mostrar graficas en el programa de base. El mismo procedimiento anterior se utiliza para los instaladores de ADODB y BASE. Por facilidad se recomienda eliminar los números de la parte final de los directorios (dejándolos solamente como jpgraph, adodb y base).

Para que funcione correctamente es necesario cerciorarse que se esté ejecutando el servidor apache con los siguientes comandos:

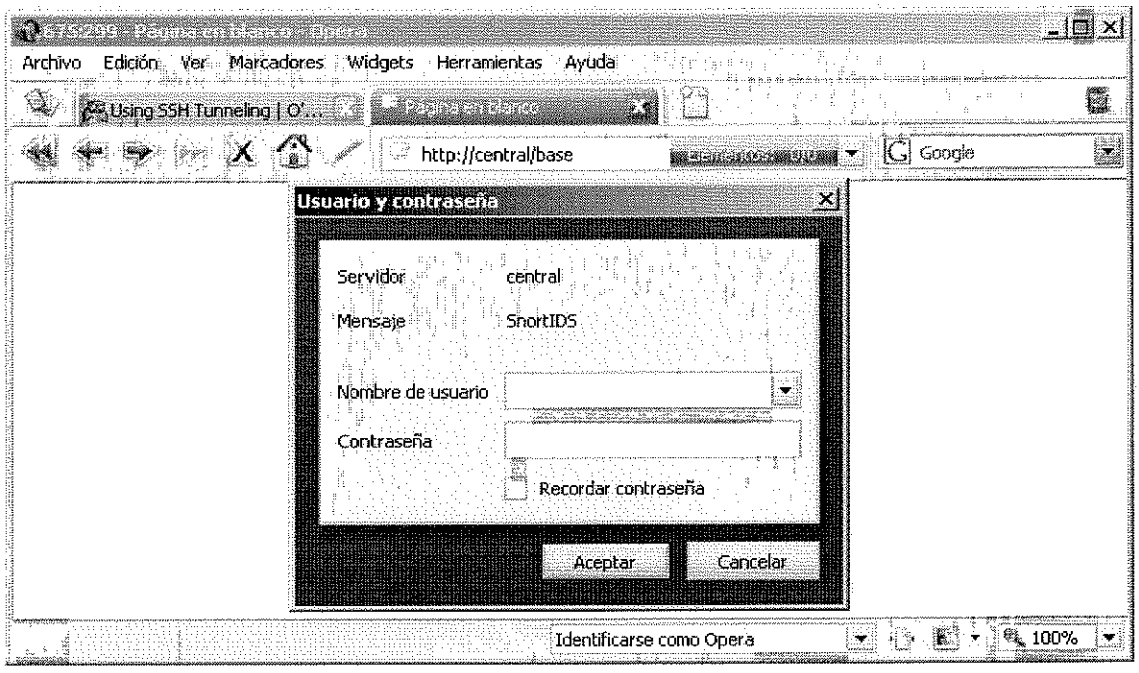
```
chkconfig httpd on
service httpd start
```

2.1 Uso y Configuración de BASE

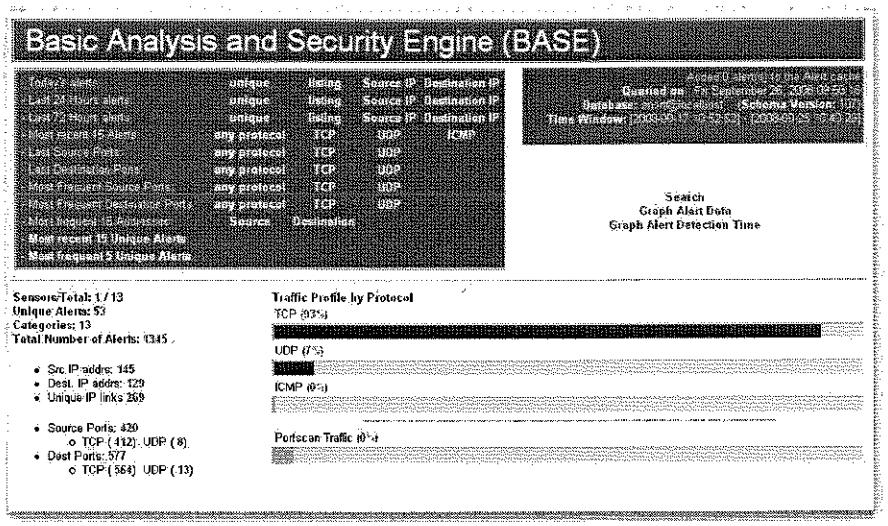
Para poder accesar a la interfaz de BASE, es necesario abrir cualquier navegador de Internet e introducir la dirección IP del equipo en el que se encuentra la interfaz BASE seguido por /base, como a continuación se indica:

```
148.225.232.162/base/
```

Una vez se establezca la conexión con el servidor, se despliega una ventana preguntando por el nombre de usuario y contraseña para acceder a la interfaz de BASE, como se aprecia en la imagen siguiente:



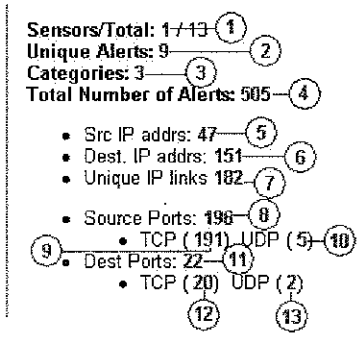
Una vez autenticados como usuarios legítimos, se muestra la página principal de BASE:

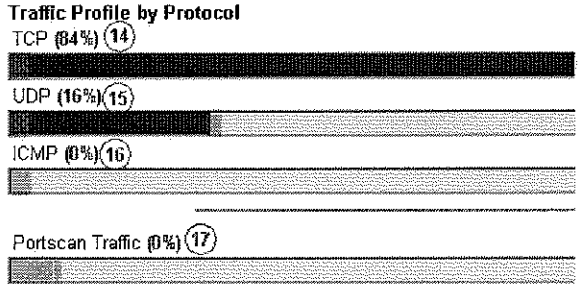


En esta pantalla se nos muestra por medio de gráficas de barras el tráfico registrado agrupado por protocolo, así como también el tráfico por puerto y las ligas para una serie de reportes predeterminados del tráfico detectado por BASE.

2.2 Reportes Predeterminados

En la pantalla principal de BASE, podemos identificar fácilmente los siguientes enlaces:





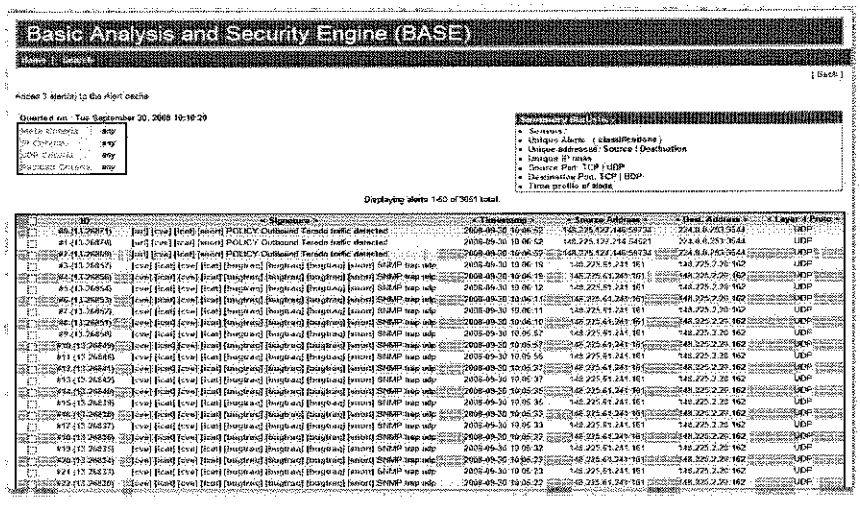
Cada número de los arriba señalados corresponde a un enlace a un reporte diferente, explicados a continuación:

1. **Sensors/Total**.- Las alertas son agrupadas dependiendo del nodo que las detectó.
2. **Unique Alerts**.- Agrupa las alertas que correspondan al mismo comportamiento (firma) sin importar la fuente o destino.
3. **Categories**.- Agrupa las alertas dependiendo de su clasificación.
4. **Total Number of Alerts**.- Muestra todas las alertas de la Base de Datos.
5. **Src. IP addrs.**- Ordena y agrupa las alertas basándose en la dirección IP fuente de las mismas.
6. **Dest. IP addrs.**- Ordena y agrupa las alertas basándose en la dirección IP destino de las mismas.
7. **Unique IP links**.- Ordena y agrupa las alertas basándose en la relación IP fuente – IP destino.
8. **Source Ports.**- Agrupa las alertas dependiendo del puerto utilizado en la IP fuente.
9. **TCP**.- Igual que la anterior, pero sólo muestra puertos del protocolo TCP.
10. **UDP**.- Igual que (8), pero sólo muestra puertos del protocolo UDP.
11. **Dest Ports.**- Agrupa las alertas dependiendo del puerto utilizado en la IP destino.
12. **TCP**.- Igual que la anterior, pero sólo muestra puertos del protocolo TCP.
13. **UDP**.- Igual que (11), pero sólo muestra puertos del protocolo UDP.

14. **TCP**.- Muestra todas las alertas registradas basadas en el protocolo TCP.
15. **UDP**.- Muestra todas las alertas registradas basadas en el protocolo UDP.
16. **ICMP**.- Muestra todas las alertas registradas basadas en el protocolo ICMP.
17. **Portscan Traffic**.- Muestra todas las alertas registradas relacionadas con el escaneo de puertos.

Para ver un reporte más detallado y específico del tráfico de cada puerto le podemos dar clic al porcentaje que se muestra enseguida al lado derecho de cada nombre del protocolo, y así nos muestra la siguiente pantalla.

Al hacer clic en cualquiera de los reportes, se nos presenta una página como la siguiente:

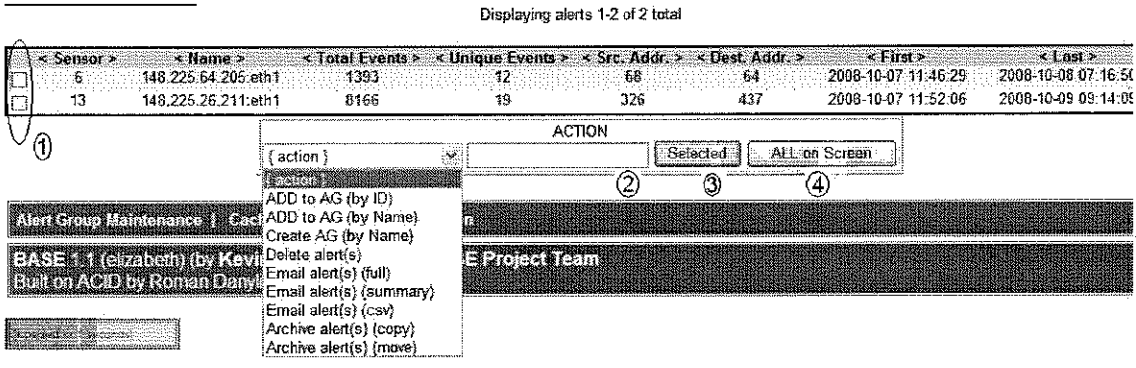


- **ID:** La primera columna sirve para identificar cada alerta asignándole un número automáticamente.

- **Signature:** La segunda columna muestra e identifica el tipo de alerta que se generó y muestra enlaces a páginas de Internet que poseen documentación sobre la alerta..
- **TimeStamp:** La tercera columna muestra el día y la hora en que fue detectada dicha alerta.
- **Source Address**: Muestra la dirección IP y el puerto donde se originó el paquete que causó la alerta.
- **Dest. Address:** Muestra la dirección IP y el puerto en el que se recibió el paquete que causó la alerta.

En el recuadro que se encuentra en la parte superior derecha de la pantalla se muestran ligas a los reportes que se pueden acceder desde la página principal explicados anteriormente, en los cuales también se muestran los resultados de las búsquedas hechas en la pagina principal.

En la parte inferior de los reportes se muestran las siguientes opciones:



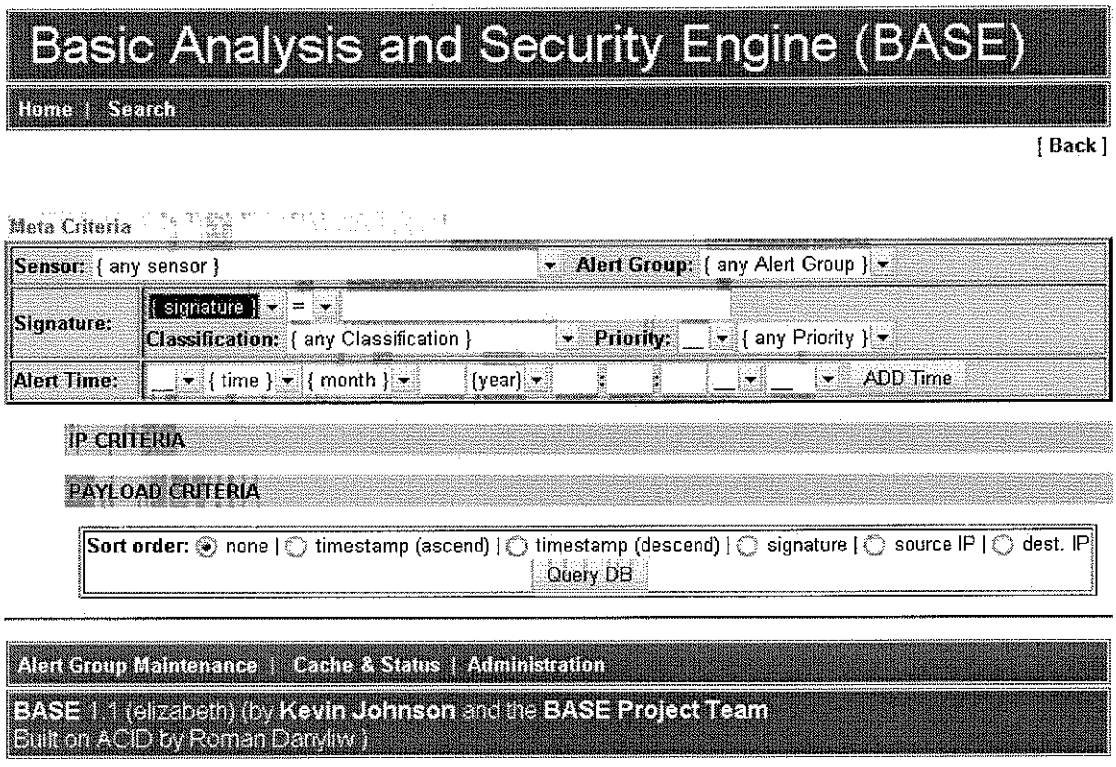
El recuadro ACTION te permite hacer cada una de las siguientes acciones:

- ADD to AG (by ID), esta opción te permite agregar una o varias alertas a un grupo de alertas (AG por sus siglas en inglés) especifico, para seleccionar las alertas que desea agregar puede dar clic en las cajas de verificación (1), las cuales se encuentran del lado izquierdo del recuadro. Una vez seleccionadas las alertas, se procede a escribir el número de identidad (id) del grupo de alertas en el cuadro de texto (2). Si prefiere agregar todas las que se muestran en pantalla, dé clic en el botón ALL on Screen (4) o también se puede optar por la opción de agregar las alertas marcadas con el botón selected(3).
- ADD to AG (by name), funciona esencialmente como el anterior, pero la diferencia radica en que en vez de introducir el número identificación del grupo de alertas, se introduce el nombre del grupo.
- Create AG, permite crear un grupo de alertas especificando el nombre del grupo en el recuadro de texto.
- Delete alert(s), permite borrar todas las alertas ya sean las seleccionadas con el botón selected(3) o todas las alertas mostradas en pantalla con el botón (4).
- Email alerts (full), envía todas las alertas seleccionadas con todo el contenido completo del mismo una dirección de correo, el cual tiene que ser escrito en el cuadro de texto(2) y presionar el botón correspondiente.
- Email alerts summary, permite enviar por correo un resumen de las alertas seleccionadas en el recuadro, especificando también el correo electrónica en el cuadro de texto.

- Email alerts (csv), envía un correo electrónico con todas las alertas generadas en forma de tabla, en donde las columnas se presentan separada por comas, para la ayuda visual y de consulta de las alertas.
- Archive alerts (copy), permite copiar las alertas seleccionadas a la dirección que se indica en el cuadro de texto(2).
- Archive alerts (move), permite mover las alertas seleccionadas a la dirección que se indica en el cuadro de texto(2).

2.3 Búsqueda

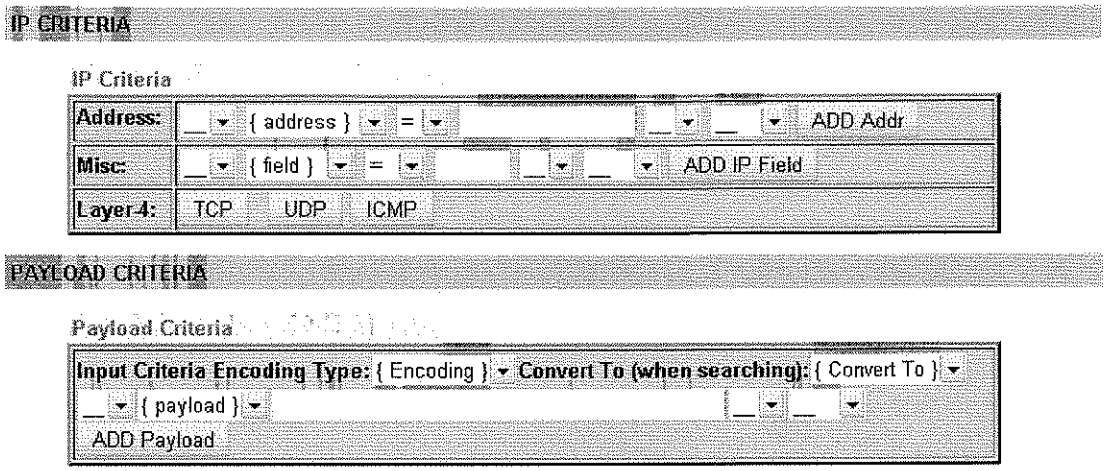
BASE cuenta con una interfaz de búsqueda de alertas a la que se puede acceder al hacer clic sobre el enlace "Search" de cualquier pantalla. La interfaz es la siguiente:



- Sección Sensor: En este campo se delimitan los resultados de la búsqueda a las alertas detectadas por el sensor especificado.

- Campo Alert Group: Seleccionando un grupo de alertas, se filtran los resultados a las alertas contenidas dentro del grupo.
- Sección Signature: Se subdivide en dos renglones. En el primero se puede seleccionar la búsqueda por nombre de alerta. Con esto se buscan las alertas en cuyo nombre aparece el texto especificado. En el segundo renglón podemos especificar la clasificación y prioridad de las alertas a buscar.
- Sección Alert Time: Aquí se debe especificar el rango de fechas de las alertas a buscar, empezando por cambiar el valor del primer campo a "(". Luego se selecciona si la fecha de captura de las alertas debe ser mayor, menor, igual o diferente de la fecha especificada y se procede a introducir la fecha. Para agregar más opciones de tiempo y fecha, se selecciona "AND" u "OR" en el último campo y se da clic en "ADD TIME".
- Por último, en "Sort Order" se selecciona cómo se han de organizar las alertas: si empezando por alertas más viejas, las más recientes, por firma, IP fuente, IP destino o ninguna.

Al hacer clic en IP CRITERIA y PAYLOAD CRITERIA aparecen nuevas opciones adicionales para la búsqueda:



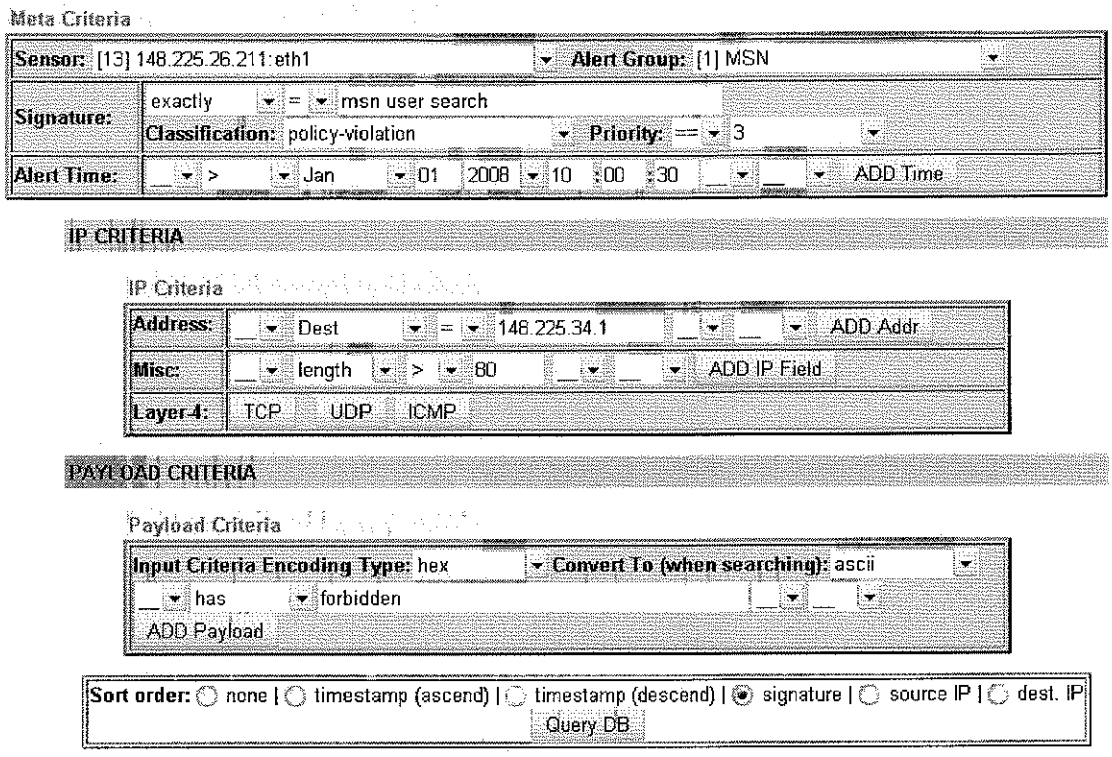
IP Critera.-

- Address: sirve para determinar los detalles sobre la dirección de fuente o destino (o ambas) de las alertas a buscar.
- Misc: Opciones varias como TOS, TTL, ID, offset, chksum, etc.
- Layer-4: Sirve para determinar si el protocolo de las alertas a buscar es TCP, UDP o ICMP.

Payload Criteria.-

- Esta sección sirve para buscar cadenas de texto o hexadecimales específicas dentro del paquete. Si se utiliza esta opción se debe especificar en qué tipo de codificación se va a buscar y si se debe cambiar de codificación al compararlo con el texto que se introduzca.

Por ejemplo, si ejecutáramos la siguiente consulta:



Los resultados mostrados obedecerían las siguientes características:

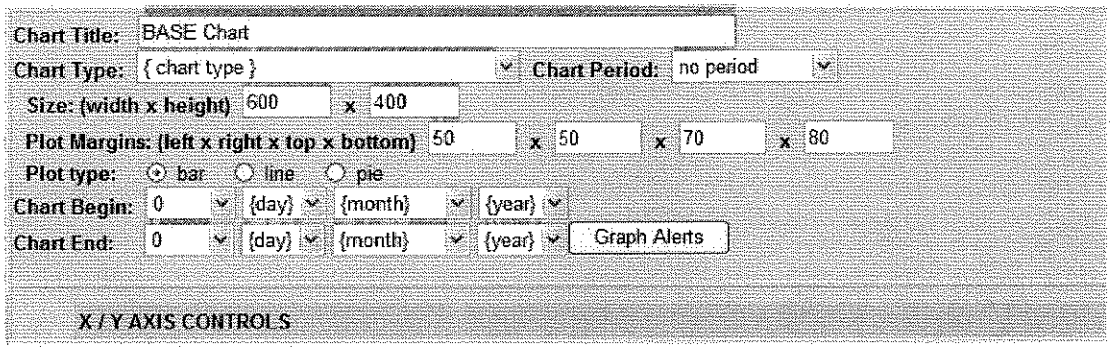
Solamente alertas detectadas por el sensor 148.225.26.211 y que sean parte del grupo de alertas MSN, dentro del nombre de alerta deben tener exactamente el texto "msn user search", estar clasificadas como "policy-violation" de prioridad 3 y la fecha de detección debe ser más reciente que 1 de enero de 2008 a las 10:00 hrs con 30 segundos. La dirección IP de destino debe ser 148.225.34.1 y la longitud del paquete debe ser mayor que 80. Por último, dentro de su codificación ASCII debe tener el texto "forbidden".

2.4 Graph Alert Data

Por medio de esta opción podemos graficar todas las alertas que se hayan generado en snort para poder comprender mejor en qué lapso de tiempo fue donde

ocurrieron más alertas y el número de las mismas que se presentaron. También las graficas sirven como una excelente ayuda visual para ver e interpretar grandes cantidades de información y así hacer la información generada por snort más comprensible.

En la siguiente imagen se muestra la interfaz de las graficas de alertas.



La opción de Chart Title es solamente para denotar el título de la gráfica que se va a realizar.

- Chart Type: sirve para denotar los datos que se quieren graficar y entre estas opciones están: tiempo en horas, tiempo en días, tiempo en meses, dirección IP origen, dirección IP destino, puerto UDP destino, puerto UDP origen, alertas por clasificación y sensores. Todos estos datos son siempre comparados contra el número de alertas. Al aparecer la gráfica, el número de alertas siempre se muestra en el eje 'Y', mostrando así los demás datos en el eje 'X'.
- Chart Period: sirve para establecer el rango de tiempo en que se van a graficar las alertas, permitiendo escoger de entre las siguientes opciones:

- ✓7 (a week), funciona para graficar todas las alertas generadas en una semana, es decir, muestra 7 días en la gráfica numerados de 0 a 6 y muestra el número de alertas generadas por día.
- ✓24 (whole day), grafica cada una de las 24 horas del día y dice cuántas alertas se generaron por hora.
- ✓168 (24x7), muestra los resultados de cada una de las horas en un rango de una semana y muestra el número de alertas generadas en cada hora.

•Size: en los cuadros de texto se denota el tamaño en píxeles de la imagen de la gráfica, el primer número establece el tamaño horizontal y el segundo el vertical.

•Plot Margins: aquí se indican los márgenes que va a tener la gráfica dentro de la imagen.

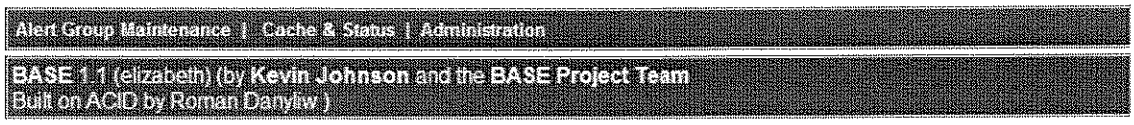
•Plot type: denota el tipo de gráfica que se desea generar, bien puede ser de barras, de pastel o de líneas.

•Chart begin: aquí se selecciona desde dónde se desea que se empiece a graficar, para esto se tiene que denotar el día, el mes y el año para que de esa manera se marque el inicio del rango de la gráfica.

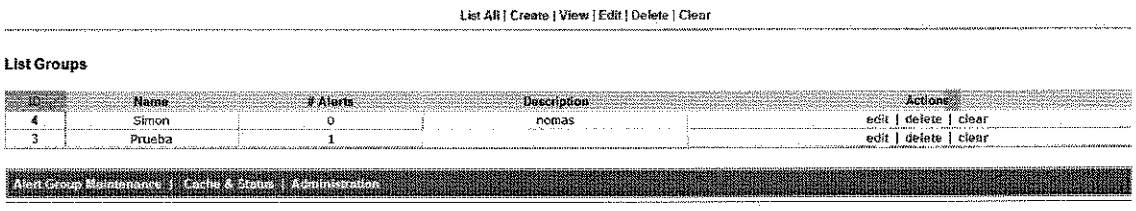
•Chart end: aquí se selecciona hasta dónde se quiere que llegue el rango de la gráfica, es decir se selecciona el último día que va a abarcar la grafica con sus respectivas alertas.

2.5 Menús de Administración

La siguiente imagen muestra 3 menús los cuales se encuentran en la parte inferior de cualquiera de las páginas o reportes de BASE:

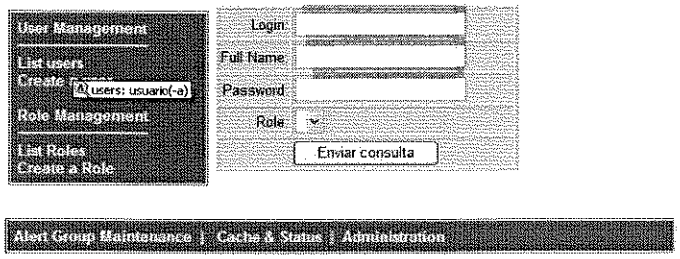


Alert Group Maintenance: Nos ayuda a llevar un control sobre todos los grupos de alerta y también nos permite crearlos, modificarlos, borrarlos, listarlos todos o borrar reglas que hayan sido añadidas un grupo de alertas en especifico.



Cache & Status, es un estado actual del sistema, es decir, dicta todas las características actuales del sistema tales como la versión de PHP, el sistema operativo, el estado actual de la base de datos en mysql, permite reparar tablas en la base de datos, así como también el total de eventos detectados durante toda la ejecución del snort hasta la fecha y ver o actualizar todas las direcciones IP detectadas como fuentes o destino en snort.

La sección de Administration es para llevar un control de usuarios y permite listar todos los usuarios registrados en el sistema, así como crear un usuario para darle acceso al sistema.



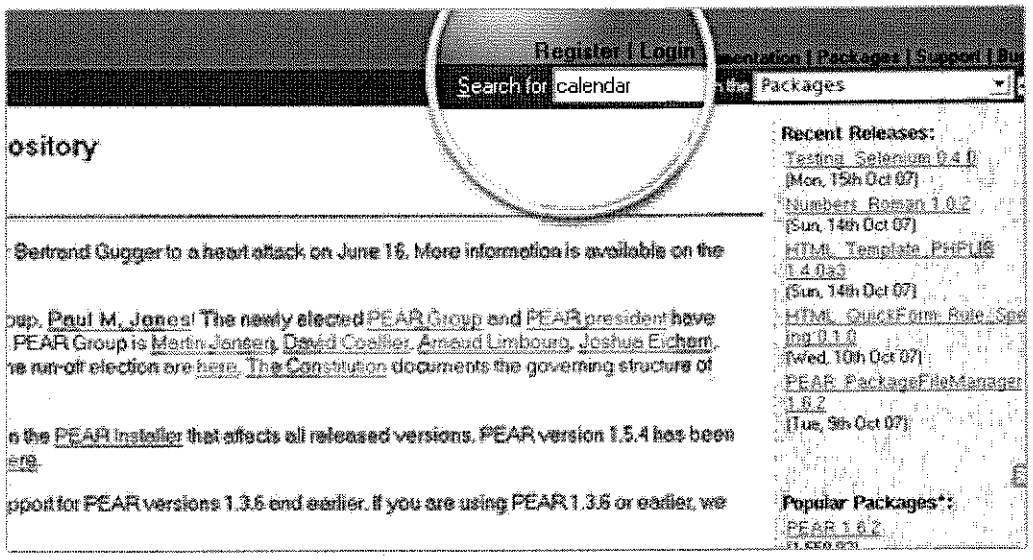
Gracias a esto se pudo establecer un sitio seguro con los passwords de cada una de las cuentas de usuario, siendo la cuenta del administrador la mas importante, la cual puede hacer modificaciones a las reglas de snort para el correcto funcionamiento del mismo.

Es importante mencionar que solo debe existir un administrador de cuenta de usuario, para evitar los problemas de configuración y que una persona solamente lo pueda controlar.

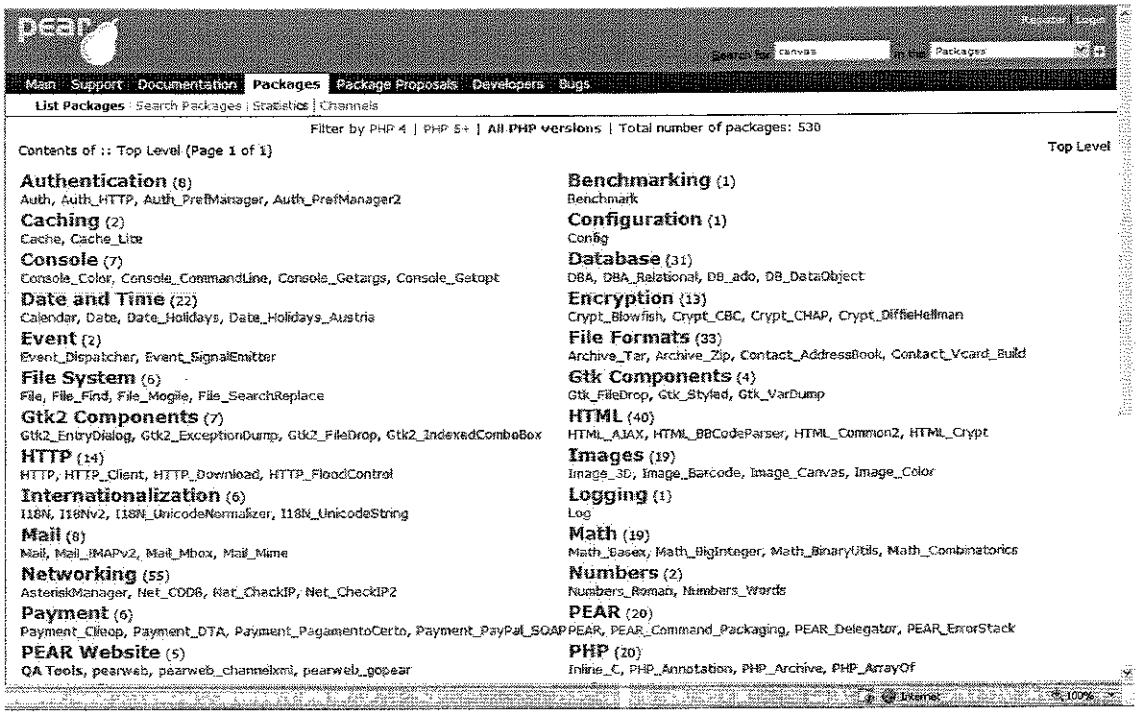
Complicaciones al Instalar Pear

Pear, es un paquete dentro de la distribución de linux, que permite instalar las aplicaciones que son necesarias para programa de monitoreo de redes snort, en cuyo caso se tuvo que actualizar en el sistema operativo fedora basado en linux, para poder realizar las graficaciones correspondientes en el snort.

Para realizar la instalación de paquetes mediante Pear, bajamos los paquetes necesarios en la pagina http://pear.php.net/ en donde buscamos un paquete llamado image canvas , necesario para la generación de imágenes de graficas en snort.



Una vez hecho esto, nos aparecerán por catalogo cada uno de los paquetes coincididos en el portal, y de aquí nos vamos a la opción Images, en el cual se contienen la gran mayoría de los archivos necesarios para hacer funcionar el graficado de los resultados de alertas del snort. Hay que tener cuidado de que paquetes están relacionados con los que vamos a bajar, ya que si no se instalan, el programa no podrá correr las graficas.

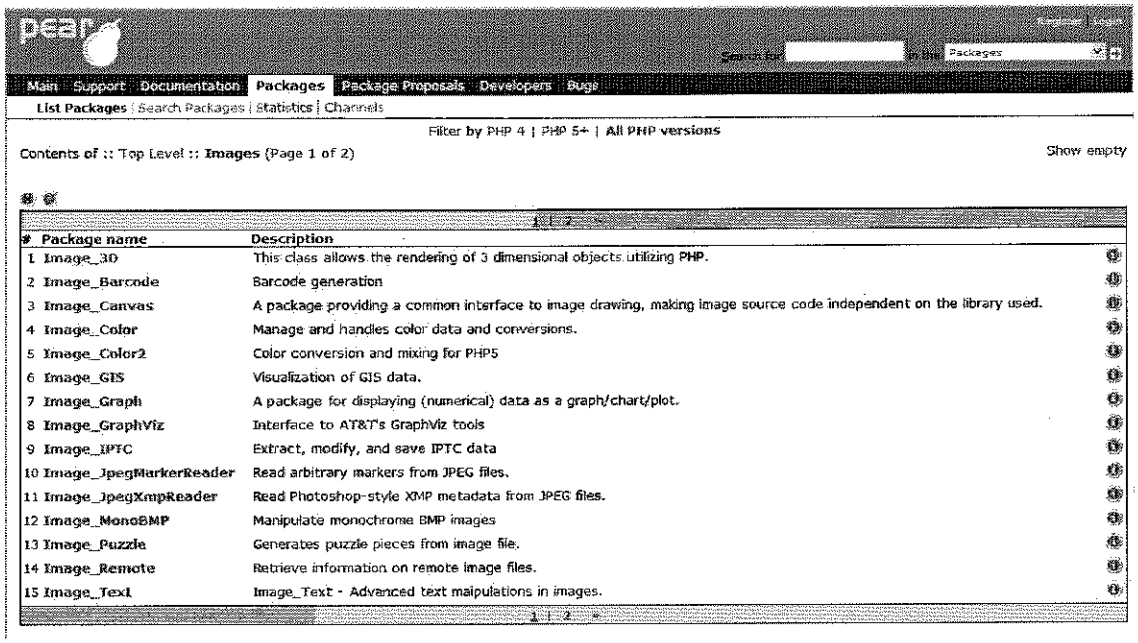


Entrando a la opción graphs se despliegan los paquetes utilizados en general para graficar en php, como se muestra en la siguiente imagen la lista. De aquí vamos a bajar los siguientes paquetes los cuales son:

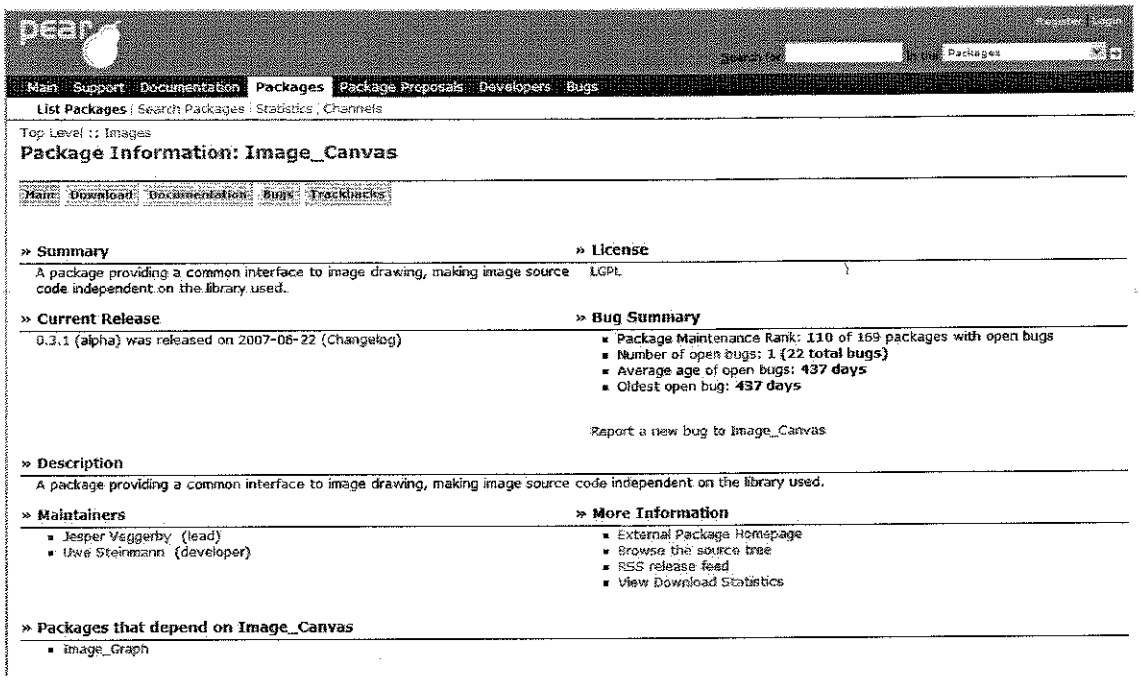
- Image 3D
- Image Barcode
- Image Color
- Image Graph
- Image Text
- Image Color 2
- Image GraphViz

Al instalar cualquiera de estos paquetes te va a pedir otro de los listados aquí, ya que están relacionados y uno no puede funcionar si no esta el paquete al que se le relaciona en la instalación. Por ende la lista se muestra en un recuadro, cuando

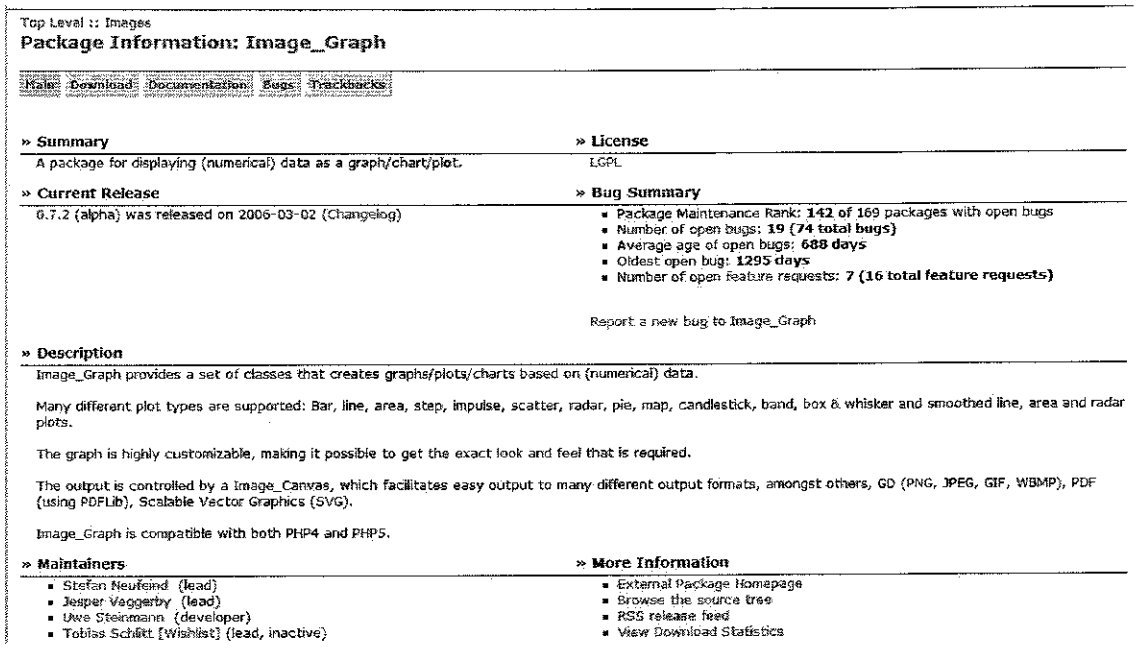
realizamos la búsqueda dentro del portal de pear, como lo muestra la siguiente imagen.



Una vez que hayamos hecho clic en cualquiera de los paquetes mencionados arriba, se nos muestra toda la información del paquete, como su contenido y a que paquete esta relacionado, el cual es lo mas importante. A continuación se muestra la información del paquete image canvas, y en la sección de abajo de la imagen se puede apreciar a cual paquete esta relacionado o depende de el.



En la sección current release, le damos al numero 0.31 que esta con verde para bajar el paquete al ordenador. Si no vamos a la sección de la dependencia que se encuentra en la parte inferior de la imagen, esta el nombre o posibles nombres de los paquetes que están relacionados. Si le damos clic en el nombre nos despliega la información del dicho paquete igual que en el paquete anterior, tal y como se muestra en la siguiente imagen.



Top Level :: Images

Package Information: Image_Graph

Main Download Documentation Bugs Trackbacks

» Summary

A package for displaying (numerical) data as a graph/chart/plot.

» License

LGPL

» Current Release

0.7.2 (alpha) was released on 2006-03-02 (Changelog)

» Bug Summary

- Package Maintenance Rank: **142** of 169 packages with open bugs
- Number of open bugs: **19 (74 total bugs)**
- Average age of open bugs: **688 days**
- Oldest open bug: **1295 days**
- Number of open feature requests: **7 (16 total feature requests)**

Report a new bug to Image_Graph

» Description

Image_Graph provides a set of classes that creates graphs/plots/charts based on (numerical) data.

Many different plot types are supported: Bar, line, area, step, impulse, scatter, radar, pie, map, candlestick, band, box & whisker and smoothed line, area and radar plots.

The graph is highly customizable, making it possible to get the exact look and feel that is required.

The output is controlled by a Image_Canvas, which facilitates easy output to many different output formats, amongst others, GD (PNG, JPEG, GIF, WBMP), PDF (using PDFLib), Scalable Vector Graphics (SVG).

Image_Graph is compatible with both PHP4 and PHP5.

» Maintainers

- Stefan Neufeind (lead)
- Jesper Veggerby (lead)
- Uwe Steinmann (developer)
- Tobias Schlitt [Wishlist] (lead, inactive)

» More Information

- External Package Homepage
- Browse the source tree
- RSS release feed
- View Download Statistics

Si se fijan, el paquete Image Graph, mostrada en la imagen, no contiene paquetes en los cuales depende, por lo cual se procede a instalar en el servidor para la graficación.

Una vez bajados los paquetes se proceden a descomprimir con el siguiente línea de comando:

tar –xf **<nombre de archivo>**

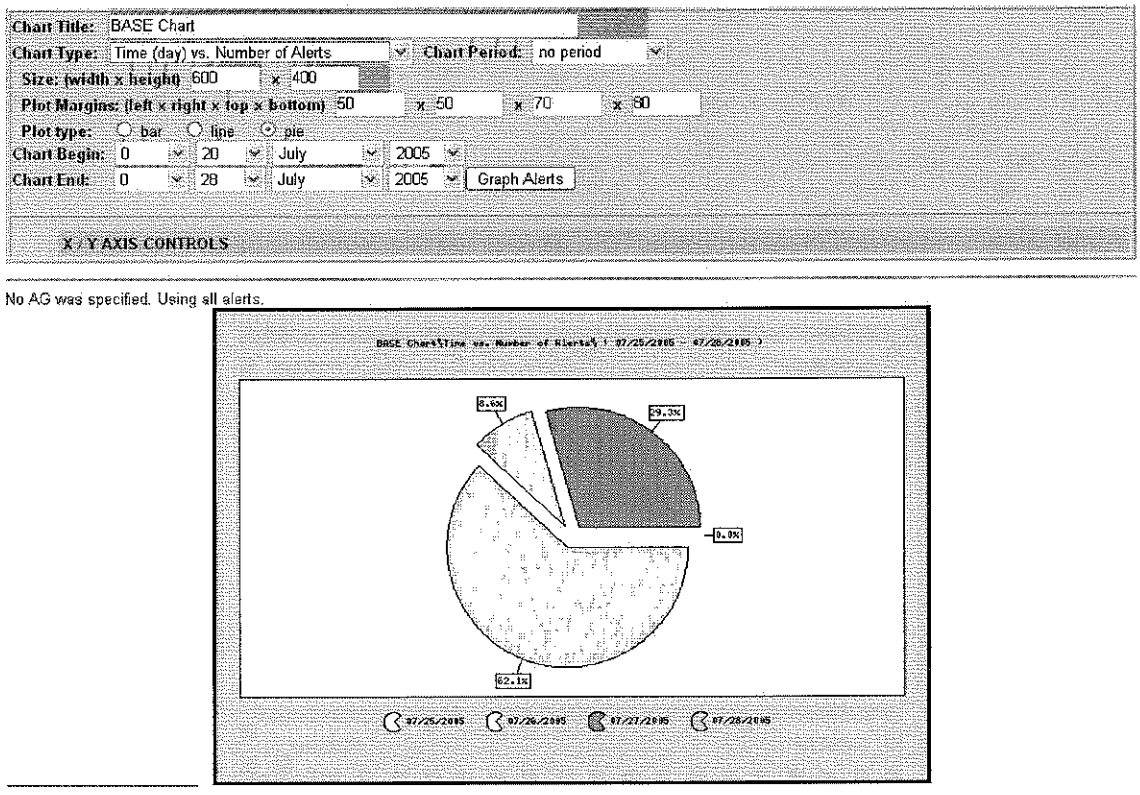
* Si el comando falla, cambiar –xf por –zxf. Si ambos fallan, volver a descargar el archivo.

Después de descomprimirlo se procede a instalarlo con las siguientes líneas de comando:

./configure

```
make
make install
```

Con esto los paquetes ya quedan instalados en el sistema operativo de fedora para la graficación de snort. Ahora nos podemos dirigir a la interfaz de base en el navegador y dirigirnos a la sección de graficación para darnos cuenta de que las graficas ya se realizan. Un ejemplo se muestra en la siguiente imagen.



También las instalaciones de pear se pueden hacer vía consola, sin tener que utilizar la página de pear para poder bajarlos. Un ejemplo seria la instalación de image graph, Para instalarlo vía consola, se necesita estar como root e introducir las siguientes líneas de comandos:

/usr/local/php/bin/pear install Image_Color
/usr/local/php/bin/pear install Log
/usr/local/php/bin/pear install Numbers_Roman
/usr/local/php/bin/pear install http://pear.php.net/get/Numbers_Words-0.13.1.tgz
/usr/local/php/bin/pear install http://pear.php.net/get/Image_Graph-0.3.0dev4.tgz

Con estos comandos se baja y se instala a la vez el paquete image canvas usando fedora core 3. Una vez que el sistema se encuentra completo, es una herramienta muy poderosa y muy útil para la Universidad de Sonora campus Hermosillo. Los servidores siguen siendo utilizados hasta la fecha por el departamento de informática.

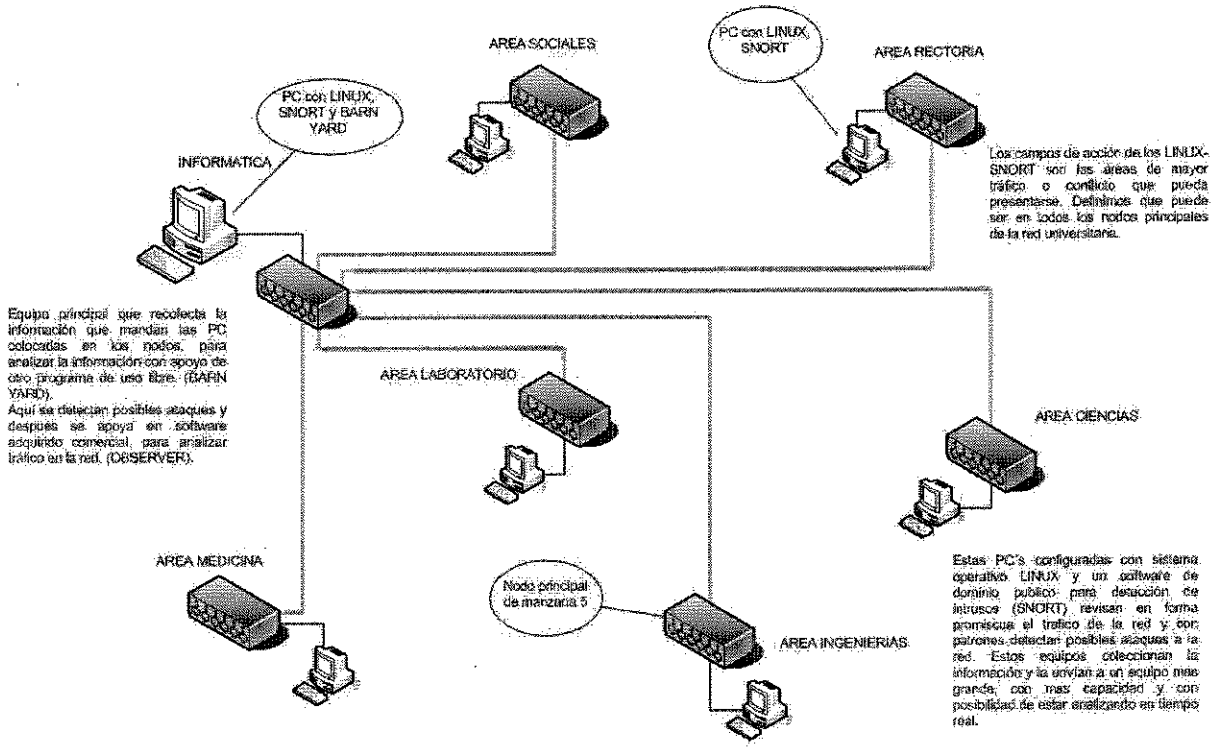
Snort no solo se utiliza en empresas y redes grandes, sino que también lo pueden usar en redes caseras o en proveedores de servicio de Internet en caso de tener problemas de robo de ancho de banda.

Los IDS son una parte muy importante en la prevención de ataques, constituyen una primera barrera que nos puede ayudar a corregir fallos de seguridad o a recopilar información acerca de un posible futuro atacante. Este documento está orientado fundamentalmente a la construcción de un Detector de intrusos casero utilizando Snort, es por ello que no se utiliza ninguna herramienta propietaria, con lo cual además de salirnos gratis tendremos un IDS libre.

Snort es la parte fundamental de esta guía. No obstante es el detector de intrusos en sí, y el resto del software de está guía está encaminada a la mejor y mas comprensible lectura de las alertas que Snort proporciona. Snort puede descargarse gratuitamente desde la web oficial (http://snort.org) aunque probablemente para cualquier distribución de Linux haya binarios disponibles en formato rpm.

RESULTADOS, PLANOS, GRÁFICAS, PROTOTIPOS Y PROGRAMAS

Figura 1 .- Red de Snort en la Unidad Campus Hermosillo



PROYECTO MONITOREO DETECCIÓN DE INTRUSOS (SNORT)

Figura 2 .- Cronogramas de las Actividades Realizadas

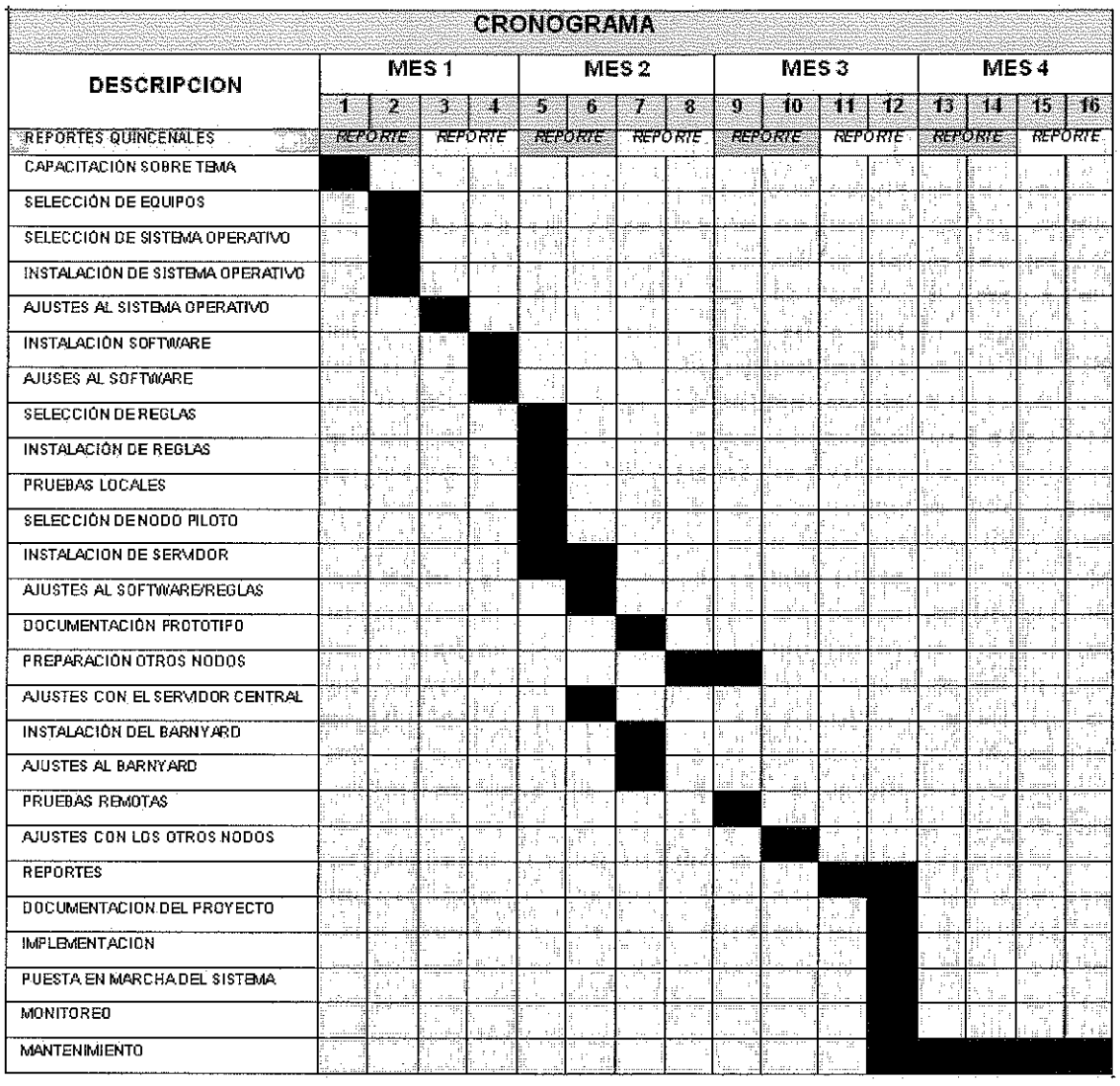


Figura 3.- Convenio de Confidencialidad de practicas profesionales

UNIVERSIDAD DE SONORA
DIRECCION DE INFORMATICA
Teléfonos (662)2-592124 y 25, 2-592224 y 28, Fax (662)2-592223

CONVENIO DE CONFIDENCIALIDAD

QUE SUSCRIBEN POR UNA PARTE EL AREA DE REDES Y TELECOMUNICACIONES DE LA DIRECCIÓN DE INFORMATICA EN LA UNIVERSIDAD DE SONORA, REPRESENTADO POR SU SUBDIRECTOR DEL ÁREA, ING. ARNOLDO FRANCISCO VIDAL ROMERO, A QUIEN EN LO SUBSECUENTE SE DENOMINARA "UNISON" EN SU CALIDAD DE RECEPTOR DE SERVICIO SOCIAL Y POR LA OTRA EL SUSCRITO _____, EN SU CALIDAD DE PRESTADOR DE [redacted] A QUIEN EN LO SUBSECUENTE SE DENOMINARA EL "PRESTADOR"

DECLARACIONES

I. La **"UNISON"** declara que debido al carácter de los compromisos adquiridos, para la formalización de un convenio y/o contrato con _____, para la realización de los objetivos y alcances del proyecto *"MONITOREO A LA RED CAMPUS HERMOSILLO"* a establecer sobre el concepto de: ANÁLISIS DE TRÁFICO EN LA RED, El **"PRESTADOR"** se compromete bajo un código de ética profesional a no divulgar por ningún medio, ni de cualquier modo hacer conocer a personas ajenas y extrañas a la **"UNISON"** cualquiera de los conocimientos al tema y al posible proyecto sujetos de interés comercial y/o propiedad intelectual que con motivo de las tareas profesionales que ejerza llegara a saber.

III. Ambas partes están interesadas en firmar este acuerdo secreto a fin de mantener salvaguardados sus intereses, por lo tanto suscriben lo consignado en las siguientes

CLAUSULAS

1a. Toda la información proporcionada por la **"UNISON"** relativa al objeto principal de este acuerdo, será tratada con estricta confidencialidad por el **"PRESTADOR"**

2a. El **"PRESTADOR"** queda obligado a no divulgar a terceros la información proporcionada por la **"UNISON"** objeto de este acuerdo.

3a. El **"PRESTADOR"** no podrá publicar los trabajos de interés académico derivados del mismo; en caso de que la divulgación se considere de interés comercial. Y sólo podrá publicarlos bajo la autorización expresa y por escrito de la **"UNISON".**
4a. Las anteriores obligaciones por parte del **"PRESTADOR"** estarán sujetas a las disposiciones contenidas en la ley de profesiones reglamentaria del Art. 5 constitucional, y demás aplicables sobre la información confidencial.

BLVD. LUIS ENCINAS Y ROSALES, COL. CENTRO, C.P. 83000
HERMOSILLO, SONORA, MEXICO
http://www.uson.mx
email: informatica@uson.mx

Figura 4 .- Continuación de Contrato de Confidencialidad

UNIVERSIDAD DE SONORA
DIRECCION DE INFORMATICA
Teléfonos (662)2-592124 y 25, 2-592224 y 25, Fax (662)3-592213

5a. El incumplimiento de este acuerdo por parte del **"PRESTADOR"** de [redacted] lo hará acreedor a las sanciones civiles y penales que resultaran de la violación de este acuerdo y obligación de ética profesional.

6a. Este acuerdo de confidencialidad tiene una vigencia de 5 años contados a partir de la fecha en que la **"UNISON"** entregue la información mencionada.

7a. Para la interpretación y cumplimiento de este acuerdo, las partes se sujetan a las leyes y tribunales competentes en la Ciudad de Hermosillo, Sonora, renunciando a cualquier otro fuero que pudiera corresponderles por razón de sus domicilios presentes o futuros.

El presente acuerdo se firma por duplicado en la ciudad de Hermosillo, Sonora, a los _____ días del mes de _____ del año de 20___.

_____	_____
ING. ARNOLDO FRANCISCO VIDAL ROMERO	
Sub Director de Redes y Telecomunicaciones UNISON	Prestador de [redacted]

BLVD. LUIS ENCINAS Y ROSALES, COL. CENTRO, C.P. 83000
HERMOSILLO, SONORA, MÉXICO
http://www.uson.mx
email: informatica@unison.mx

Fortalezas y Debilidades

Fortalezas

El haber llevado materias optativas relacionadas con los sistemas operativos en el estudio de la carrera universitaria, permitió el entendimiento práctico de lo que se implemento mediante sistemas operativos basados en Linux como lo fue en este caso con la distribución de Fedora.

El conocimiento del hardware y equipamiento de los equipos, se realizó gracias a los conocimientos previos obtenidos durante el transcurso de la carrera. Los conocimientos se obtuvieron durante la realización del servicio social en los laboratorios de cómputo en el departamento de industrial de la universidad de sonora.

Las instalaciones en red de los nodos y sus configuraciones que se hicieron fueron gracias a los conocimientos adquiridos por los cursos de cisco en el estudio de la carrera.

Las configuraciones de base de datos en MySQL y la configuración del apache para levantar el sitio de monitoreo se facilitaron gracias a las clases de lenguajes de programación en el estudio de la carrera.

Debilidades

Problemas en la configuración de las tarjetas de Ethernet en el entorno de Linux con la distribución de Fedora, debido a la escasez de una o algunas materias que nos formarán dentro del entorno grafica de software libre.

Hubo algunos problemas en la instalación de ciertos paquetes que necesitaba el programa de monitoreo, para dar su buen funcionamiento, por lo cual se tuvo que buscar como instalarlos.

Oportunidades y Recomendaciones

Las oportunidades hoy en día para los ingenieros en sistemas se encuentran altas ya que los sistemas de computo así como las redes de datos se están volviendo en algo necesario para las empresas, incrementándose así las oportunidades de los ingenieros en sistemas de información, ya que con la aptitud y conocimientos en programación y redes computacionales lo hacen una personas apta y capaz para poder confrontar los problemas y situaciones difíciles de las empresas en cuestiones de esas áreas.

Las especialidades o materias optativas de nuestra carrera nos permiten potencializar nuestro conocimiento en algo más específico y así poder acatar las altas demandas del mercado hoy en día. También debido a que llevamos materias de la carrera ingeniería industrial, nuestro enfoque se amplia dando mas posibilidades.

Mi recomendació sería que los maestros apoyen más los alumnos en encontrar empresas en donde desarrollar sus prácticas profesionales y los orienten en escoger cuál sería su mejor opción y de qué manera sacar mayor provecho de ello.

De ser posible, tratar de desarrollar experiencia profesional durante el transcurso de la carrera, no solamente durante la realización de las practicas profesionales, sino desde antes, para que cuando se llegue a la culminación de los estudios sea mucho mas fácil conseguir empleo, teniendo así experiencia laboral y aparte el apoyo que la universidad brinda al egresado.

Seria bueno que los alumnos tuvieran un tutor designado para la estancia profesional en su carrera, con el fin de aclarar cualquier duda que tenga y así mezclar los conocimientos que el tutor le provee con los que esta adquiriendo en la empresa en donde el alumno desarrolla su estancia profesional.

Conclusiones y Recomendaciones

Hoy en día las empresas se están volviendo más competitivas y cada vez aumenta el grado de conocimiento y de preparación que un profesional debe de tener para conseguir empleo y competir en el mercado laboral.

Es por eso que las prácticas profesionales es un parte integral para el alumno, ya que conlleva la puesta en práctica de los conocimientos que adquirió durante el desarrollo de su carrera y al mismo tiempo adquiere también experiencia laboral que le permitirá al alumno mejor probabilidades de conseguir un buen empleo.

El conocimiento nuevo que adquirí durante el desarrollo de las prácticas fue abundante y muy importante, ya que aplique algunos de los conocimientos que adquirí durante el estudio de mi carrera, junto con el conocimiento que desarrollé dentro de la empresa.

El alumno se debe de esforzar al máximo en la realización de las practicas ya que dependiendo de su esfuerzo es muy probable que consiga desarrollar su carrera profesional dentro de la empresa en la cual esta desarrollando sus practicas, es decir, conseguir que le den un empleo.

El departamento de informática nos brindó la oportunidad de realizar nuestra estancia profesional con ellos, y por ello les estoy muy agradecido ya que en este mismo departamento muchas actividades de las que se realizan forman parte integra nuestra

formación como ingenieros en sistemas de información y nos brindó la oportunidad de crecer aun mas tanto en los conocimientos como el carácter.

Estudiar una carrera es difícil, pero a la vez importante y satisfactoria ya que cumples con tus objetivos propuestos y avanzas un paso más de conseguir un empleo bien remunerado.

Referencias Bibliograficas y Virtuales

http://www.snort.org/about_snort/

http://www.infosecwriters.com/text_resources/pdf/snort_base_fc3.pdf

http://sourceforge.net/project/showfiles.php?group_id=103348

http://base.secureideas.net/about.php

www.informaticavip.com.ar/pdf/Articulo_Sniffers.pdf

www.frikis.org/documentos/cisco_router2.pdf

http://www.snort.org/docs/faq/1Q05/node86.html

https://fedoraproject.org/wiki/Fedora_Project_Wiki

http://es.wikipedia.org/wiki/C%C3%B3digo_libre