IMPLEMENTACIÓN DE UN SISTEMA DE DETECCCION DE INTRUSOS BRINDANDO SEGURIDAD A LOS SERVIDORES DE LA EMPRESA "TENNIIS S.A"

ANDRÉS SANTAMARÍA CASTAÑO
ESTEBAN ACOSTA RUIZ

INSTITUCIÓN UNIVERSITARIA DE ENVIGADO
FACULTAD DE INGENIERÍA
TECNOLOGÍA EN GESTIÓN DE REDES
ENVIGADO
2012

IMPLEMENTACIÓN DE UN SISTEMA DE DETECCCION DE INTRUSOS BRINDANDO SEGURIDAD A LOS SERVIDORES DE LA EMPRESA "TENNIIS S.A"

ANDRÉS SANTAMARÍA CASTAÑO
ESTEBAN ACOSTA RUIZ

Trabajo Presentado Como Requisito Parcial en el cuarto Semestre de la Tecnología en Gestión de Redes

ASESORES
MARTA LUCIA HERNANDEZ
DIEGO ALEXANDER DUQUE MARIN
HECTOR FERNANDO VARGAS MONTOYA

INSTITUCIÓN UNIVERSITARIA DE ENVIGADO
FACULTAD DE INGENIERÍA
TECNOLOGÍA EN GESTIÓN DE REDES
ENVIGADO
2012

1. RESUMEN

Cada vez más los sistemas de cómputo se convierten en parte fundamental de la vida diaria de las personas y compañías, incrementado el intercambio de información a través de métodos virtuales que permiten simplificar y facilitar las comunicaciones superando cada vez más las capacidades de almacenamiento de toda la información.

Con el paso del tiempo el tema de la seguridad para los sistemas de información ha ido ganando importancia, por lo cual a medida que han surgido avances en materia de la tecnología ,también han surgido nuevas formas e ideas de asegurar la información, buscando al máximo conservar y la confidencialidad de esta evitando el acceso a personas inescrupulosas que pueden alterar ,destinar la información para su uso propio o buscando fines diferentes para los que fue creada.

Teniendo en cuenta que en la actualidad el número de amenazas que puede presentar un sistema es demasiado alto, las mismas necesidades de buscar proteger la información dentro de un sistema o red han llevado a la creación de programas que permiten llevar un control y tener una mejor protección de la información.

La protección de la información va ligada a las necesidades de una persona o cada empresa en especial, de las exigencias o necesidades propias es que surgen las soluciones para poder brindar seguridad a una red o sistema como tal. Proporcionando más confianza en el momento de utilizar la información ya que tiene la certeza de que esta es procedente de un lugar seguro.

Para poder mitigar los riesgos en materia de seguridad dentro de un sistema o red, es necesario conocer de los diferentes sistemas que permiten brindar seguridad a los mismos, siendo importantes en este tema los sistemas de detección de intrusos (IDS), los firewall, los sniffer y teniendo en cuenta que estos son los que permiten llevar un control de seguridad en un sistema de una forma preventiva, ayudando al análisis de incidencias ,ataque y fallas que presente una red en el tema de seguridad.

2. ABSTRACT

Each time more computer systems become essential part of daily life of individuals and companies, increasing the exchange of information through virtual methods to simplify and facilitate communications beating every time more storage capacities of all information.

time over the issue of security for information systems has become increasingly important, so have emerged as advances in technology have also created new forms and ideas to ensure the information, looking for the most and preserve the confidentiality of preventing access to unscrupulous people who may alter, set aside the information for their own use or looking for other purposes for which it was created.

Given that at present the number of threats that may present a system is too high, the same needs to seek to protect the information within a system or network have led to the creation of programs that allow you control and have a better Protection information.

The protection of information is linked to the needs of a person or each company in particular, the requirements or special needs arise is that solutions to provide security to a network or system itself. Providing more confidence when using the information as it is certain that this is from a safe place.

In order to mitigate the security risks within a system or network, you must know the different systems that provide security to allow them, to be important in this matter the intrusion detection systems (IDS), firewalls, sniffer and considering that these are the ones allowed to carry a security check on a system of preventive, helping the analysis of incidents, assault and failure to present a network security issues.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

3. INTRODUCCION

La seguridad en las redes de comunicaciones se a vuelto pilar fundamental en los servicios de red que poseen las grandes empresas, debido a la gran prioridad que ha tomado el tratamiento de la información en el mundo entero ya que está utiliza este medio para ser compartida, movilizada o analizada, con esto surge la necesidad de crear e implementar sistemas que permitan asegurar y proteger la transferencia y privacidad de los datos desde sus orígenes hasta el destino deseado, con todo este esquema se requiere de un sistema de detección de intrusos como elemento imprescindible para la seguridad de la red de datos.

Con estos sistemas se podrán monitorear y detectar eventos que estén ocurriendo en la red de datos y así poder analizarlos para buscar posibles vulnerabilidades que afecten parte o toda la infraestructura de red de la compañía, y así elaborar propuestas para dar solución a estos problemas minimizando el impacto que puede ocasionar y el riesgo de manipular la información a través de estos medios.

Con este proyecto se busca implementar un IDS(sistema de detección de intrusos) para el análisis de la red de la compañía TENNIS S.A. basándose en la utilización del software SNORT como herramienta que facilita el control, análisis y registros de los datos que circula en la red.

Es importante para la implementación de SNORT, tener bien definidas las áreas de la red que se desean monitorear, y el lugar donde se desea instalar para así evitar información que confunda el analista debido a falsos positivos y alertas innecesarias que pueden cargar o saturar el proceso de recolección de información y que este se encargue luego de definir las reglas de firewall que sean necesarias para proteger o asegurar las comunicaciones.

4. PLANTEAMIENTO DEL PROBLEMA

Los sistemas de comunicación actuales son utilizados para el transporte de información en empresas y para los usuarios, a través de equipos informáticos y electrónicos por medio de recursos propios de la infraestructura de red y de protocolos que son utilizados para comunicar aplicaciones por medio de mensajes que controlan las comunicaciones evitando de algún modo la perdida de conexión y entregando los datos de forma integra y segura, estos procesos de comunicación son a veces afectados por personas indeseadas dentro de las redes corporativas o personales, afectando el normal desempeño de las redes informáticas que no están protegidas por dichas amenazas.

Los atacantes pueden ser detectados por movimientos dentro de los sistemas ya que pueden ocasionar ataques de denegación de servicios o también por accesos a archivos confidenciales o inhabilitando el acceso a otros servidores u otros puntos de la red de datos, una vez implementados los sistemas de detección de intrusos se puede identificar mas fácilmente amenazas anteriores o posibles amenazas que debido a la complejidad de la información arrojada es necesario la actualización de los sistemas mientras se logra analizar todo este material.

Muchos de los fallos son ocasionados por los mismos dispositivos pero principalmente son provocados por la falta de seguridad dentro de la red en donde el desconocimiento o la confianza pueden provocar perdida de información muy importante o daños a otros usuarios que hacen uso de recursos de la red, es por eso que una red debe estar siempre protegida por un sistema de detección de intrusos(IDS) y un firewall que minimice los riesgos de tener información compartida en una red de datos ya que con esto solo los host o usuarios tendrán acceso a lo que realmente necesitan, manteniendo el correcto funcionamiento y desempeño de todos los sistemas de información.

Cada día es necesario tener con mayor protección las redes y los sistemas de computo por los cuales cruza información importante dentro de una empresa, buscando ofrecer mayor seguridad y respaldo a la información; evitando amenazas que comprometan la integridad de la información ocasionando pérdidas lógicas y físicas por el uso mal intencionado de personas ajenas a la organización o con intereses personales .

Es necesario un sistema de firewall para evitar al máximo violar los parámetros internos de seguridad de la información dentro de la empresa Tennis S.A.

El respaldo y ante todo la protección y la seguridad de la información dentro de un sistema o red es indispensable en todo momento teniendo en cuenta que tipos de amenazas o vulnerabilidades pueden estar presentes dentro de la red interna de una organización buscando al máximo mantener la confidencialidad, disponibilidad e integridad de los datos.

¿Qué ventajas trae para una compañía la implementación de un sistema de seguridad que permita llevar un control y análisis de la red interna?

5. OBJETIVOS

5.1GENERAL

Implementar un sistema de detección de intrusos (IDS) que permita la detección de paquetes de red de usuarios no autorizados o que deseen obtener privilegios no deseados dentro de la red de la compañía.

5.2ESPECÍFICOS

- Prevenir problemas de seguridad disuadiendo posibles ataques.
- Eliminar los riesgos de ataques o posibles intrusiones dentro de la red de datos de la compañía.
- Realizar revisiones periódicas del estado de la seguridad de la red.
- Reducir gradualmente el nivel de riesgo de seguridad de la red.
- Detectar ataques que no son identificados por el resto de sistemas de seguridad de la compañía.
- Proveer información útil sobre las intrusiones que se están produciendo.

6. JUSTIFICACION

Los principales problemas de los sistemas informáticos se encuentran en la seguridad que estos tienen, las malas políticas y las malas practicas son motivos por los cuales se vuelven cada vez mas vulnerables, siempre debe ser de vital importancia conservar la integridad de los datos que son almacenados electrónicamente en dispositivos creados para dicho fin, lo que hace que cada vez tomen más importancia los datos guardados para luego ser accedidos y tratados por personal calificado y autorizado.

Para el análisis y tratamiento de los datos e información es necesario tener equipos y herramientas que procesen la información recolectada, además se debe tener personal con conocimientos sobre amenazas, que monitoren los sistemas y riesgos informáticos, Se debe contar con personal que realicen la instalación y configuración lo que obliga a que se automaticen tareas y así reducir el tiempo de respuesta cuando aparezcan incidentes de seguridad.

El constante aumento de las amenazas informáticas a través de internet y el no cumplimiento de las políticas de seguridad aumentan los riesgos provocando ser victimas de ataques informáticos, tanto en la parte interna como externa, para llevar a cabo un plan de seguridad existen sistemas que ayudan a fortalecer el procesamiento de la información asegurando cada una de las áreas, que se necesiten proteger, herramientas que pueden ser libres o que tienen un costo pueden ser enfocadas a un solo sistema en particular o multiplataforma.

Ya los sistemas operativos traen consigo herramientas básicas y un poco complejos que permiten llevar una bitácora del sistema donde lleva registros de procedimientos, uso de recursos, movimiento de los usuarios, errores que se generan cuando algo falla o cuando se inicia el sistema, pero en realidad no permiten llevar un seguimiento o analizar cuando el sistema a sido vulnerado ya que no existe una metodología que permita saber que elementos están comprometiendo la integridad del sistema, además de registrar un volumen considerable de información, sin clasificar, imposible de revisar minuciosamente por parte del administrador del sistema, perdiendo mucho tiempo en la toma decisiones y causando riesgo ante cualquier problema de seguridad . Esta información puede pasar a un segundo plano ya que dichos registros pueden ser comprometidos por un atacante o personas no autorizadas al sistema, modificándolos y perdiendo integridad en la información que el sistema pueda arrojar pasando por desapercibido cualquier indicio de cambios que se pueda presentar, lo que puede comprometer todo el sistema afectándolo. Otro

elemento importante son las llamadas al sistema que también son registradas y que informan sobre cualquier comportamiento de los ejecutables .

La información descrita anteriormente permite llevar un escenario ideal para la detección de intrusiones ya que se necesita detectar y reconocer las variaciones que tienen los sistemas en su estructura tanto de archivos como del sistema en general, programas, procesos ejecutados, permisos recursos consumidos, cargas del sistema, etc. lo que exige un alto consumo de recursos y una disminución del rendimiento del sistema, todas estas herramientas de detección pertenecen al sistema o instalarse de manera opcional permitiendo mas organización de la información almacenada, reducción de tiempos de respuesta y mayor legibilidad para analizar la información ante cualquier incidente informático.

7. MARCO TEORICO

7.1. ACERCA DE LINUX [1]

Es un sistema operativo que consta de varios programas fundamentales, que permiten al computador o servidor comunicarse y recibir instrucciones de los usuarios; dichas instrucciones pueden ser leer y escribir datos en el disco duro, cintas, e impresoras; controlar el uso de la memoria; y ejecutar otros programas. Hay que tener en cuenta que la parte más importante de este sistema operativo es el núcleo. En este caso para GNU/Linux como es conocido popularmente, es necesario saber que Linux es el núcleo del sistema operativo.

Linux está modelado como un sistema operativo tipo Unix. Desde sus comienzos, fue diseñado como un sistema multi tarea y multi usuario. Debido a esto Linux marca unas grandes diferencias que lo hacen distinto como sistema operativo entre todos los que se encuentran hoy en día en el mercado, teniendo en cuenta que nadie es dueño de Linux gracias a que su desarrollo esta relacionado con el software libre donde un grupo de personas voluntarias ayudan a que este todos los días sea mas eficaz y a que sus herramientas sean mas robustas logrando así el crecimiento de Linux como sistema operativo.

Su origen comienza en 1984 cuando la Free Software Foundation (Fundación de software libre, N. del t.) empieza a desarrollar un sistema operativo libre Unix, llamado GNU.

El proyecto GNU ha sido el encargado de desarollar diversas herramientas de software libre para ser utilizados por Unix™ y sistemas operativos tipo Unix como Linux. estas herramientas permiten desarrollar tareas tan simples como copiar o eliminar ficheros del sistema, o tan avanzadas como escribir y compilar programas .

Es de gran importancia resaltar que Linux es un sistema operativo estable que permite ejecutar varios programas al mismo tiempo y que tiene un nivel de seguridad muy alto, debido a esto a tene gran demanda en el mercado.

---

[1] Debían.org. Guía de instalación de Debian GNU/Linux. Disponible en: http://www.debian.org/releases/stable/amd64/ .9 de abril 2012

7.2. DEBÍAN COMO HERRAMIENTA[2]

Es una de las herramientas GNU, con el núcleo Linux, y perteneciente al software libre, siendo esta una distribución de Linux que está formada por un gran número de paquetes y cada uno de estos contiene ejecutables, scripts, documentación e información de configuración. Siendo esta una distribución de Linux de alta calidad, estable y escalable. La instalación puede configurarse fácilmente para cumplir diversas funciones desde firewall reducidos al mínimo y servidores de red para alto rendimiento, etc.

Debían fue la primera distribución de Linux en incluir un sistema de gestión de paquetes para permitir una fácil instalación y desinstalación del software, también fue la primera que podía actualizarse sin necesidad de una reinstalación.

En la actualidad continúa siendo líder en el desarrollo de Linux. Su proceso de desarrollo es un claro ejemplo de lo bien que puede funcionar el modelo "Open Source" para tareas tan complejas como construir y mantener todo un sistema operativo.

Lo que más distingue a Debían de otras distribuciones GNU/Linux es su sistema de gestión de paquetes, otorgando al administrador del sistema un control total sobre los paquetes instalados, buscando proteger paquetes individualmente de forma que no sean actualizados e incluso puede indicar al sistema de gestión de paquetes qué programas ha compilado usted mismo y qué dependencias cumplen.

En la parte de seguridad debían trae con el un sistema de parches de seguridad que se actualizan automáticamente para así buscar proteger el sistema contra "caballos de Troya" y otros programas malévolos, teniendo en cuenta que los servidores debían tienen la capacidad de verificar que los paquetes sean provenientes de encargados auténticos en cuanto al desarrollo de este, con el fin de evitar al máximo ser vulnerado por códigos maliciosos.

[2] Debían.org. Guía de instalación de Debian GNU/Linux.disponible en: http://www.debian.org/releases/stable/amd64/ .9 de abril 2012

7.3. GENERALIDADES DE LA SEGURIDAD EN UN SISTEMA DE INFORMACIÓN[3]

El termino seguridad esta relacionado a un servicio que garantiza que el funcionamiento de todas las máquinas pertenecientes a una red sea óptimo, además buscando que todos los privilegios de los usuarios sean concebidos adecuadamente para evitar que personas no autorizadas intervengan en el sistema con fines malignos o que los usuarios realicen operaciones involuntarias que puedan dañar el sistema. Buscando asegurar los datos mediante la previsión de fallas, garantizando que no se interrumpan los servicios.

En todo tipo de sistema o red este tema es de gran importancia teniendo en cuenta que busca la protección de todos los datos que cruzan por una red o que se encuentran implantados en un sistema, la seguridad se puede clasificar de dos formas:

- Seguridad activa, esta tiene como fin proteger ante cualquier posible intento de abuso a la protección de una red o de un sistema, un ejemplo de esta seguridad puede ser un firewall que se encarga de filtrar el acceso a servicios en ciertas conexiones evitando vulnerabilidades desde un servicio cualquiera.

- Seguridad preventiva es la que se encuentra implementada en un sistema y se encarga de informar si hay incidencias de seguridad por medio de alertas pretendiendo proteger el sistema, un ejemplo muy claro es un sistema de detección de intrusos.

Es una realidad que en la actualidad las redes son atacadas y vulneradas, conociendo que cada año se incrementa la velocidad de expansión, la habilidad de ejecución y el daño que produce cualquier tipo de ataque, por lo tanto, es muy necesario llevar un estudio para logra la elaboración de tácticas que permitan tener un grado adecuado para la protección, buscando saber cuales son los objetivos propios de la seguridad .Es necesario mencionarlos y tenerlos en cuenta:

- Brindar integridad a los datos de cualquier sistema asegurando que la información no va a tener modificación alguna por personas ajenas o no autorizadas .

[3] Mayra Pazmiño; Jorge aviles;cristina abad. Captura y análisis de los ataques informáticos que sufren las redes de datos de la ESPOL, implantando una honeynet con miras a mejorar la seguridad informática en redes de datos del Ecuador.disponible en: https://www.dspace.espol.edu.ec/bitstream/123456789/4203/1/6722.pdf. 9 de abril 2012

- Buscar la disponibilidad de la información en todo momento garantizando la disposición de los datos a tiempo .para poder realizar cualquier petición evitando perdidas importantes en los datos.
- Manejar la confidencialidad de los datos que se encuentran asegurados en un sistema con el fin de evitar la divulgación de estos a personas ajenas.

Es de gran importancia conocer los parámetros para poder obtener una red segura, ciertos puntos que hacen referencia a lo que se debe proteger dentro de la red y de quien se debe proteger, teniendo estos dos puntos definidos se puede realizar el estudio de las herramientas necesarias para dar solución al problema de la red en cuanto a seguridad; Teniendo en cuenta que tipos de ataques ha sufrido dicha red.

7.4. TIPOS DE ATAQUES A UNA RED[4]

7.4.1.Ataque de negación de servicio (DOS): Su modo de ejecución esta en enviar un numero peticiones a las máquinas, causando así un descontrol en estas por que no son capaces de responder a todas las peticiones que han sido enviadas, provocando que las maquinas se saturen y dejen de funcionar .El programa del atacante simplemente hace una conexión en un puerto de servicio, envía la petición a el puerto y luego corta la conexión con este . Si el equipo es capaz de responder a 20 peticiones por segundo, el atacante le envía 50 por segundo, para así poder tumbar un servicio y el atacante lograr lo que desea con la red.

Hay que tener en cuenta algunos conceptos para poder reducir un ataque de denegación de servicio, estos pueden ser:

- Tener en cuenta el uso del filtrado de paquetes para poder evitar que estos entren directamente a un espacio de direcciones de red.
- Mantenerse al día con los parches de seguridad respectivos para los sistemas operativos.

7.4.2.Acceso no autorizado: Hace referencia a varios tipos de ataques que tienen como objetivo acceder a algún recurso que el equipo no debe proporcionar al atacante , este tipo de ataque tiene como fin escalar privilegios para causar daños dentro de una red, teniendo en cuenta que

[4] Matt Curtin. Introduction to network security. Disponible en: http://www.interhack.net/pubs/network-security/. 20 de abril 2012

dichos privilegios serán otorgados a cualquier usuario de una red, permitiendo que este sea el atacante.

7.4.3.Ejecución de comandos ilícitamente: Este tipo de ataque va relacionado a los usuarios que pretenden realizar un daño en la red interna de una compañía, por que debido a este el usuario puede tener acceso a los servidores buscando ocasionar un problema en estos, por medio de las líneas de comandos; para así ejecutar comandos que puedan alterar de diversas maneras el funcionamiento de todos los servidores implementados dentro de una compañía o buscar obtener violaciones de confidencialidad de la misma.

Los ataques pueden ser causales de daños lógicos o físicos dentro de una red, teniendo en cuenta que a estos van ligados un gran numero de técnicas que pueden permitir de forma rápida atentar contra la seguridad propia de la información, sistemas o en otro caso de la red siendo analizado de una forma más global; teniendo el atacante como objetivos:

- La atracción hacia lo prohibido
- El deseo de obtener dinero
- Tener reputación
- El deseo de hacer daño cuando se encarga de destruir datos o hacer que un sistema no funcione.

7.5. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

Partiendo del concepto de un sistema de detección de intrusiones se tiene como aquel sistema que permite solicitar información de diferentes fuentes de un sistema buscando alertar una posible intrusión en las redes o equipos pertenecientes a estas. Dichas alertas pueden ser debidas a que se tiene un intento de intrusión, un comportamiento poco frecuente en la red, anomalías en el comportamiento de los equipos debido a que pueden estar realizando ciertas tareas que no son de uso frecuente en la red y en ciertos casos porque viaja información que no es normalmente tratada por los servicios de la red. Es considerable decir que un sistema de detección de intrusos es un modo para el control de auditoría que permitirá realizar análisis de seguridad en cualquier tipo de sistema o red. Siendo mas una medida pro-activa y preventiva que ayuda al

administrador de red o sistema a saber cuándo hay anomalías y agujeros de seguridad o falta de protección en los sistemas que son administrados.[5]

Estos sistemas tienen como principales características:

- Detectar o monitorear los eventos ocurridos en un sistema informático o red logrando buscar intentos de ataques que puedan comprometer la seguridad de dicho sistema.
- Buscar patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre una red o equipo.
- Ayudar a la prevención alertando anticipadamente cualquier actividad sospechosa. Teniendo en cuenta que No están diseñados para detener un ataque, aunque sí pueden generar ciertos tipos de respuesta ante éstos.
- Aumentar la seguridad de un sistema, vigilando el tráfico de la red, examinando los paquetes de datos sospechosos.

Normalmente esta herramienta se integra con un firewall, el detector de intrusos es incapaz de detener los ataques por sí solo, excepto los que trabajan conjuntamente en un dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

Los IDS esta divididos en tres tipos, teniendo en cuenta que cada uno de ellos presenta funciones específicas dentro de un sistema o red. [6]

7.6. TIPOS DE IDS

7.6.1. HIDS (HOST IDS): Es aquel que protege un servidor, host o computador. Se encarga de monitorear los eventos, analizando todas las actividades con gran precisión, para así ayudar a determinar que procesos

[5] DAVID FERNANDEZ VAAMONDE .detección de intrusos en GNU/Unix. Disponible en : http://stuff.gpul.org/2003_jornadas/doc/deteccion_de_intrusos/deteccion_de_intrusos.html . 5 de marzo 2012

[6] linux party group.El Sistema de Detección de Intrusos: Snort. (Windows y Linux).disponible en : http://www.linux-party.com/modules.php?name=News&file=article&sid=6000.16 de abril 2012

y usuarios están involucrados en una acción determinada. Consiguen información del sistema como ficheros, logs, recursos, etc. para un posible análisis de incidencias.

7.6.2. NIDS (NET IDS): Es un tipo de IDS que Protege el sistema basado en la red. Actúan capturando y analizando paquetes de red, es decir, son sniffers del tráfico de red. Luego analizan los paquetes capturados, buscando patrones que supongan algún tipo de ataque.

Los NIDS cuando se encuentran bien ubicados dentro de una red pueden analizar en gran dimensión y el impacto en el tráfico suele ser pequeño. Estos analizan el trafico de red normalmente en tiempo real; No sólo trabajan a nivel TCP/IP, también en el nivel de aplicación.

7.6.3. DIDS (Distributed IDS): Es el encargado de Proteger un sistema con una arquitectura basada en cliente-servidor esta formado por un conjunto de NIDS que actúan recopilando toda la información en una base de datos central. Este tipo de sistema permite configurar con reglas específicas de control que se aplicarán a un determinado segmento de red.

Los IDS se pueden clasificar de dos formas según su tipo de respuesta en:

- Pasivos: Son aquellos IDS que notifican al administrador de la red mediante alarmas o reportes, si la red esta siendo atacada. Este tipo de IDS no actúan sobre el atacante.
- Activos: estos generan un tipo de respuesta sobre el sistema atacante o en otro caso a la fuente de ataque y permite cerrar la conexiones o enviar algún tipo de respuesta que se encuentre definida en la configuraciones.

7.7. TIPOS DE SISTEMAS DE SEGURIDAD

Los sistemas de seguridad van ligados a las exigencias y necesidades de un sistema, teniendo en cuenta el tipo de seguridad que se desea implementar.

Hay diversos elementos que pueden ayudar a la seguridad propia de un sistema, teniendo en cuenta que la seguridad esta dividida en dos tipos, activa y preventiva.

En el caso de la seguridad activa es necesario implementar sistemas que cumplan con mayores exigencias y que de cierto modo sean capaces de poder identificar un ataque y tengan la capacidad de responder al mismo.

Para este tipo de seguridad hay diferentes sistemas que permiten prestar los servicios de protección adecuada para evitar ataques a una red, estos tipos de sistemas pueden ser:

7.8. FIREWALL[7]

Es un dispositivo que filtra el tráfico entre redes. Este puede ser un dispositivo físico o un software sobre un sistema operativo. En general debe ser reconocido como una caja con dos o más interfaces de red en la que se crean una reglas de filtrado con las que se define si una conexión determinada puede formarse o no. Incluso puede ir más lejos y realizar alteraciones sobre las comunicaciones, como por ejemplo en el NAT[8](es un sistema que generalmente se utiliza para asignar una red completa (o varias redes) a una sola dirección IP con el fin de reducir el numero de direcciones IP en una sola dirección NAT, haciendo la traducción de direcciones IP internas con la dirección IP NAT facilitando que el firewall reconozca la dirección y evite que sea bloqueada)

Hoy en día un firewall es un hardware definido con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/../IP y resuelve si un paquete pasa, se altera, se cambia o se retira. Para que este funcione entre redes debe tener como mínimo dos tarjetas de red, la primera para comunicarse con el exterior y la segunda para comunicar la red interna como lo demuestra la siguiente imagen:

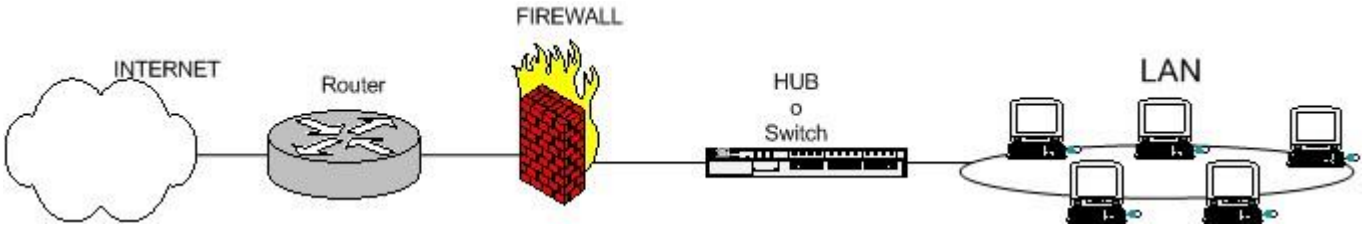


Figura 1. Arquitectura de un firewall

[7] PELLO XABIER ALTADILL IZURA. iptables manual practico.disponible en: http://www.pello.info/filez/firewall/iptables.html#2 . 5 de marzo 2012

[8]OPENBSD.traduccion de direcciones de red NAT.disponible en: http://www.openbsd.org/faq/pf/es/nat.html .10 de marzo 2012

Con este esquema se pretende proteger una red local conectada a internet a través de un router. Donde El firewall debe estar ubicado entre el router y la red local o al dispositivo que comunica con esta, en este caso puede aplicar para el router de un ISP.

Dependiendo de las exigencias y necesidades de cada red, puede implementarse uno o más sistemas de firewall para crear distintos perímetros de seguridad en referencia a un sistema. Éste puede ser denominado DMZ que es conocido comúnmente como zona desmilitarizada.

Es necesario conocer que los firewall están divididos en varios tipos de acuerdo con las necesidades y exigencias de seguridad que se deban implementar. Otro esquema es como se puede ver a continuación donde el equipo que actúa como firewall tiene tres interfaces conectadas a diferentes segmentos de la red:

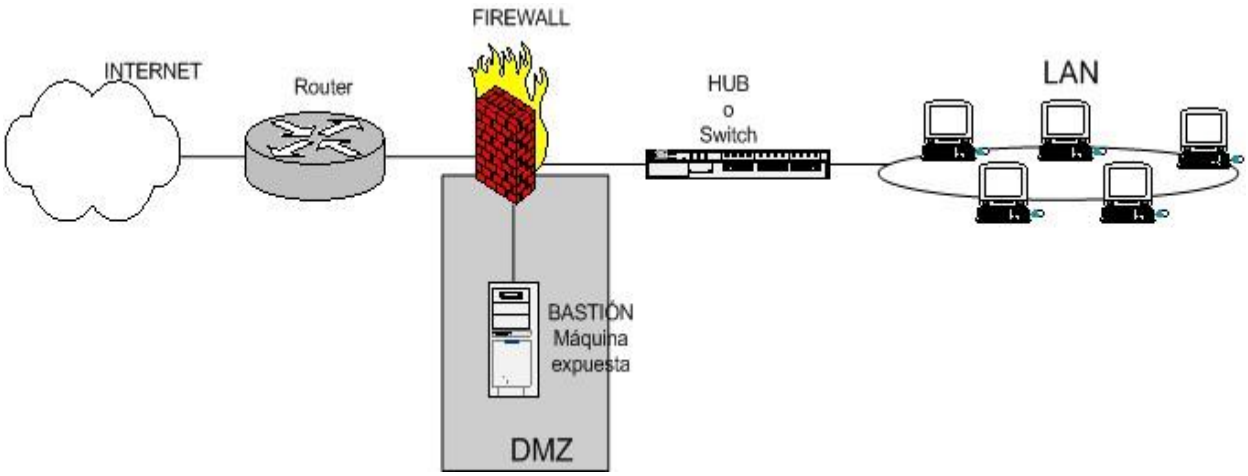


Figura 2. Arquitectura de un firewall con DMZ

En la DMZ (zona desmilitarizada) se pueden ubicarlos servidores como se necesiten. Con esta arquitectura, se permite que el servidor sea accesible desde internet de tal forma que si es atacado y se logra acceder a él, la red local sigue protegida por el firewall.

Este esquema es con el fin de que se pueda implementar doble firewall:

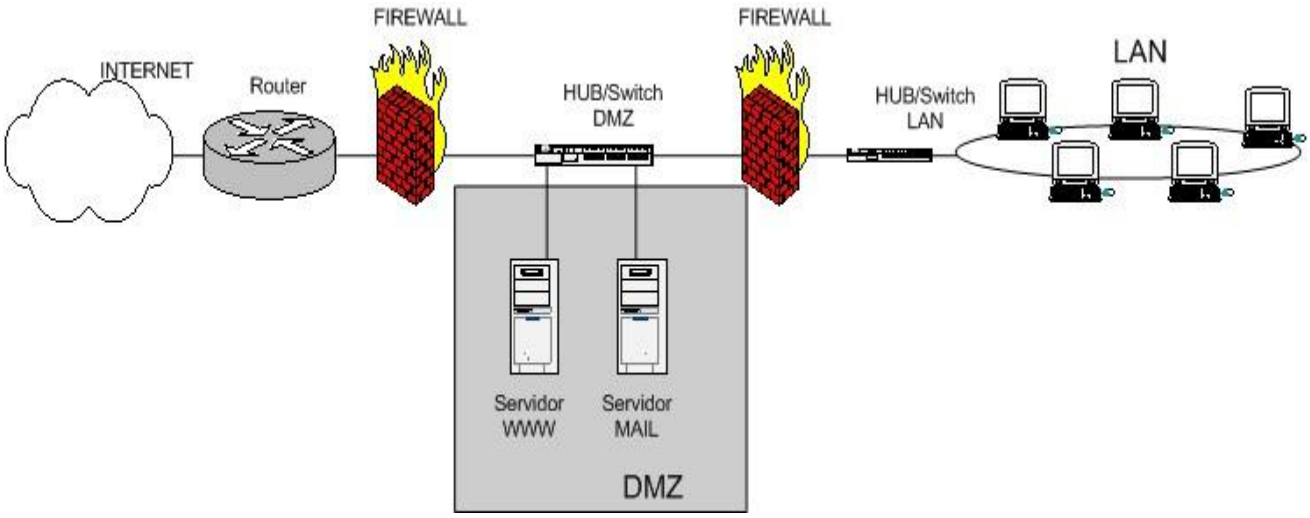


Figura 3. Arquitectura de un firewall doble

Este esquema de firewall entre red local e internet con zona DMZ es para servidores expuestos, con doble firewall.

Los firewalls se pueden usar en cualquier red. Es usual tenerlos como protección de Internet en las empresas, siendo la función de estos controlar los accesos externos hacia dentro y los internos hacia el exterior; teniendo en cuenta que esto puede hacerse adicionalmente con un proxy que también permita utilizar reglas, en un nivel más alto para poder brindar mayor seguridad dentro de la red interna de una empresa.

A continuación en la gráfica se puede observar una arquitectura que permitirá identificar como puede ser el funcionamiento de un firewall en un Pool de servidores que se encuentra dentro de una empresa y a los cuales hay que brindarles seguridad contra intrusos.

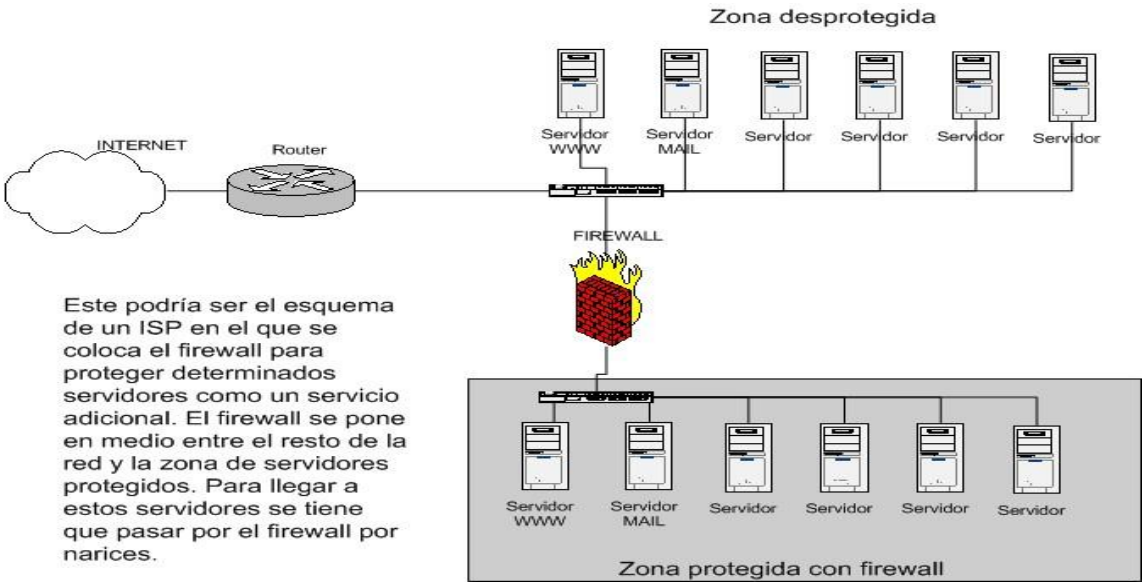


Figura 4. Arquitectura de un firewall para la protección de la DMZ

Un firewall dentro de una red constituye una especie de escudo protector de los equipos y sistemas pertenecientes a esta, teniendo como función examinar cada uno de los paquetes que traten de ingresar o salir de una red de acuerdo a las reglas que se encuentren previamente establecidas, este decide que paquetes deben pasar y cuales deben ser bloqueados . [9]

Muchos tipos de firewalls son capaces de filtrar el tráfico de datos que intenta salir de la red al exterior, evitando así que los diferentes tipos de código malicioso como caballos de Troya, virus y gusanos, entre otros, sean efectivos. El firewall actúa de intermediario entre el equipo (o red local) e Internet, filtrando el tráfico que pasa por él (Se sabe que todas las comunicaciones de internet se realizan mediante intercambio de paquetes de información).Un firewall se encarga de controlar y proteger todas las comunicaciones de un sistema.

7.8.1Tipos de firewall según el modelo OSI[10] : Existen diversos tipos de firewall pero sin duda una de las clasificaciones mas importantes serian los pertenecientes a los niveles de capa osi, teniendo en cuenta que en un primer lugar están los del nivel tres de la capa osi que seria el nivel de red o en otras palabras nivel IP en redes TCP/IP como Internet, este tipo de firewall son considerados como filtros de paquetes de cuya función es filtrar intentos de conexión atendiendo direcciones ip de origen,

[9] UNAM CERT. Firewall personales. disponible en: http://www.seguridad.unam.mx/descarga.dsc?arch=422. 1 de mayo 2012

[10] el prisma. cortafuegos-firewall . disponible en: http://www.elprisma.com/apuntes/ingenieria_de_sistemas/cortafuegos/default3.asp. 1 de abril de 2012

destino y puertos de destino de los paquetes ip; teniendo como objetivo controlar el acceso a los servidores y sistemas que se encuentran dentro de una red y en la mayoría de los casos viene implementados en routers comerciales.

En segundo lugar se pueden implementar firewall pertenecientes al nivel 4 del modelo osi, que hacen referencia al nivel de transporte en las rede TCP/IP, con este tipo de firewall se pude determinar si cierto numero de paquetes son pertenecientes a una conexión de inicio o a una conexión ya establecida.

En tercer lugar se tienen los firewall pertenecientes al nivel 7 de la capa osi, siendo estos del nivel de aplicación y actúan como proxy para las diferentes aplicaciones que se desean controlar. Además de lo anteriormente mencionado existen otro tipo de firewall.

7.8.2. Firewall de filtrado de paquetes*:* Son los que se ven utilizados en routers con reglas de filtrado de paquetes que son utilizados para conceder o denegar el ingreso de datos a una dirección fuente, dirección de destino y puerto, son utilizados como forma de segura en entornos de bajo riesgo por lo que ofrece seguridad mínima y a bajo costo, tiene como características la rapidez, la flexibilidad, y transparencia, alguna de las desventajas que presenta este tipo de firewall son:

La única referencia que tiene el router para poder otorgar un acceso o no a una red LAN son la información que se encuentra en la cabecera del paquete IP que por lo general suelen ser IP de destino, la IP de origen y los puertos.

- No protege contra “spoofing” (ó engaño) de direcciones DNS o IP.
- No manejan un sistema de autenticación confiable.
- No proporcionan buena información de registro.

7.8.3.Firewall de nivel de aplicación: Con este tipo de firewall se enfoca hacia servidores proxies que se encargan de tomar decisiones externas para examinarla y renviarlas como peticiones legitimas, teniendo en cuenta que estos tienen la capacidad de autenticar los usuario y los registros, siendo este el firewall mas seguro, proporcionado una seguridad ante el riesgo de media – alta, ya que este permite la configuración de una única dirección visible a una red externa, permitiendo que todas las conexiones de adentro hacia afuera y afuera hacia adentro pasen por este firewall.

- De cierto modo este también impide el acceso directo a una red interna.
- Si la red interna esta mal configurada o no es segura, por medio de la utilización de proxies se puede estar protegido.
- Por medio de este tipo de firewall se pueden proporcionar registros.

7.8.4.Firewall híbridos*:* Son una combinación del firewall para el filtrado de paquetes y el firewall de aplicación, teniendo en cuenta que son implementados en serie buscando maximizar la seguridad, siendo este una arquitectura ideal para la protección de los sistemas internos de una red.

7.8.5Firewall para intranet*:* Estos normalmente se encuentran entre una red corporativa y una red no segura como internet, buscando aislar una subred particular de la red corporativa total.

Estos se implementan partiendo de la necesidad que tiene la organización de tener un uso limitado de cierta información para algunos de los usuarios internos, siendo esta una información sensible o confidencial que proporciona un alto grado de responsabilidad en su utilización.

El firewall para intranet es utilizado con el fin de tener un control de acceso elevado, que soporte auditorias y registros.

7.9. IPTABLES[11]

Es un sistema de firewall vinculado al kernel de Linux que se ha desarrollado enormemente a partir del kernel 2.4 de este sistema operativo. Este no es un servidor que se inicia o se detiene, ni que se pueda caer por un error de programación, está integrado con el kernel y es parte del sistema operativo. Su funcionamiento está ligado a la ejecución del comando iptables, con el que añaden, borran, o se crean reglas. Debido a esto un firewall de iptables es un simple script de Shell en el que se van haciendo las reglas de firewall.

Como las reglas de firewall están a nivel de kernel, y a este lo que le llega es un paquete y asume que debe hacer con él, todo esto dependiendo si el paquete es para la propia maquina o para otra máquina, esto lo decide por medio de

[11] PELLO XABIER ALTADILL IZURA. iptables manual práctico. Disponible en: http://www.pello.info/filez/firewall/iptables.html#2 . 5 de marzo 2012

consultas que hace a las reglas de firewall para así saber qué hacer con el paquete según lo que se encuentra estipulado dentro de las reglas de mismo.

Así será el camino que llevara un paquete en el kernel:

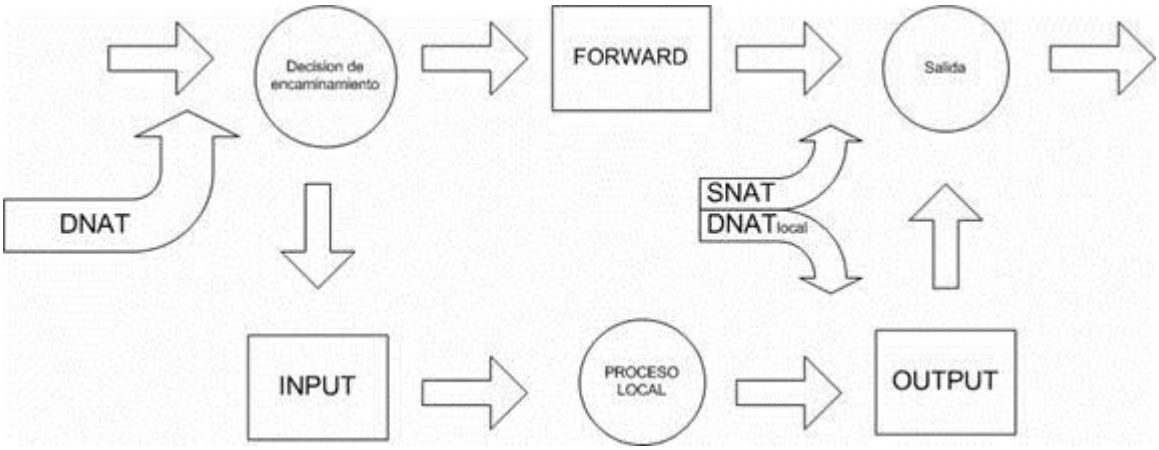


Figura 5.arquitectura del camino que lleva un paquete en el kernel de linux con iptables

Básicamente se observa si el paquete esta destinado a la propia maquina o si va para otra:

- Para los paquetes que se dirigen a la propia maquina se aplican las reglas INPUT y OUTPUT.
- Para filtrar paquetes que van a otras redes o maquinas se emplean reglas FORWARD.

Para estas tres reglas de filtrado se deben tener en cuenta antes de aplicarlas, la posibilidad de implementar las reglas de NAT que son usadas para hacer redirecciones de puertos o cambios en las IPs de origen y destino e incluso antes de estas se pueden introducir reglas de tipo MANGLE que son las destinadas a modificar los paquetes.

En iptables son utilizadas las siguientes reglas:

- MANGLE
- NAT: Reglas PREROUTING, POSTROUTING
- FILTER: Reglas INPUT, OUTPUT, FORWARD.

7.10. SHOREWALL[12]

En algunos casos es importante utilizar herramientas que permitan facilitar al administrador de la red el ingreso de las diferentes reglas de firewall por medio de iptables, esta herramienta puede ser Shorewall, la cual permite realizar la configuración de una manera mas practica y eficaz, buscando generalizar los datos en algunos ficheros de texto simple, para así crear las reglas de firewall correspondientes, a través de iptables.

Siendo Shorewall un software que facilita generar las reglas de configuración del netfilter. Es un conjunto de ficheros que se utiliza para configurar y controlar los paquetes del núcleo Linux.

Es necesario conocer que para la utilización del Shorewall hay que tener en cuenta los diferentes ficheros que este utiliza y para que sirven, a continuación serán mencionados y explicados. [13]

En primer lugar se tiene el fichero de interfaces que es en el cual se especifican todas las interfaces de red existentes dentro de un sistema, asociando a redes que vienen predefinidas en la configuración de Shorewall, siendo estas :

- net →"internet".
- loc →"red local".
- fw →"máquina que ejerce el firewall".

En segundo lugar se tiene el fichero de módulos de kernel "modules" que es donde se especifica que módulos del kernel se deben cargar.

Para un tercer lugar esta el fichero de políticas generales "policy" que es en donde se establecen las políticas de ejecución con respecto a las interfaces ya establecidas buscando aceptar o rechazar conexiones que vienen de internet o que salen para internet; para esto se utilizan los comandos Drop que es utilizado para no responder a la conexión entrante, el comando REJECT que es el que hace un rechazo activo y el ACCEPT que es el que acepta la conexión.

[12] wilmer haumani corboba. instalar firewall enlinux server con shorewall. dispinible en : http://configurarlinuxserver.com/instalarfirewallenlinuxserver.pdf . 6 de marzo 2012

[13] juanjoalvarez.net .configuracion absurdamente rapida del firewall shorewall. disponible en : http://juanjoalvarez.net/es/detail/2009/jun/25/configuracion-absurdamente-rapida-del-firewall-sho/ .8 de marzo 2012

En cuarto lugar se tiene el fichero de reglas “rules” que es en donde se especifican las reglas concretas de firewall y tiene como objetivo crear excepciones a las políticas generales, en este fichero se pueden declarar los puertos que se desean abrir para la comunicación de la red o en otro caso se puede realizar la declaración de los puertos que no se quieren filtrar.

Por ultimo está el fichero de zonas “ZONES” es donde se definen el alias(nombre de las zonas) y las descripciones para cada una de las zonas que van a ser tomadas por el firewall.

7.11. SNORT[14]

Es básicamente un sistema de detección de intrusiones (IDS), cuya funcionalidad nativa es captar el tráfico de un segmento de red. Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL.

Siendo este un sniffer de paquetes que actúa a nivel de red puede captar las transmisiones que se asemejen como potencialmente maliciosas y recolectarlas en un registro.

El snort tiene con el implementado un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida. Así mismo utiliza herramientas que le permite mostrar incidencias e informar en tiempo real, convirtiéndose en un sistema de detección y prevención de intrusos, siendo el ACID la herramienta que facilita al snort generar los reportes e incidencias.

Snort Utiliza la librería estándar libcap y el programa tcpdump para registro de paquetes. Este implementa un lenguaje de creación de reglas flexible y potente. Es posible que permita de todas las formas añadirle una serie de reglas ya creadas que permiten filtrar puertas traseras, ataques DoS, ataques web, herramientas de exploración de servidores.

[14] PIERPAOLO PALAZZOLI, MATTEO VALENZA . utilizando snort inline. Disponible en: http://snortattack.org/docs/SNORT_ES.pdf. 5 de marzo 2012

El funcionamiento de el snort esta ligado a otros servicios adicionales, buscando que esta herramienta pueda cumplir con todos los objetivos para así satisfacer todos los requerimientos necesarios de este.

Es necesario tener en cuenta que necesita de herramientas como bases de datos mysql , de un lenguaje php, de una aplicación web llamada ACID que es la encargada de gestionar y mostrar las incidencias dentro del sistema de detección de intrusiones “snort”. y en ultimo lugar un servidor web “apache”.

7.12. ACID

Teniendo en cuenta que el ACID es una aplicación web, escrita en el lenguaje php que permite acceder a toda la información que proporciona snort de manera ordenada y sencilla.

Realiza búsquedas de todo tipo en la base de datos, estas búsquedas pueden ser por ip fuente/destino, por fecha, por ataque, por protocolo, realizar informes, graficas, Además facilita el análisis de los logs. [15]

7.13. MySQL[16]

Es un sistema de gestión de bases de datos relacional, licenciado bajo la GPL de la GNU, siendo este un gestor de bases de datos considerado el mas usado en el mundo del software libre por sus ventajas en cuanto a rapidez y facilidad de uso.

Este comprende un gran número de librerías que facilitan la interacción con los diferentes lenguajes de programación, teniendo en cuenta la facilidad que este otorga para su instalación y configuración.

[15] cesar gonzales. snort+mysql+acid :sistema de deteccion de intrusos open source.disponible en : http://linuca.org/body.phtml?nIdNoticia=13 . 10 de marzo 2012

[16] DANIEL PECOS .PostGreSQL vs. MySQL .disponible en :http://danielpecos.com/docs/mysql_postgres/index.html .1 de mayo 2012

7.14. PHP [17]

Es un lenguaje de programación de alto rendimiento , diseñado para la creación de paginas web dinámicas y en el caso de snort es el encargado de realizar enlace entre el servidor web y la base de datos, permitiendo visualizar y analizar los datos de snort por medio de un servidor web.

7.15. APACHE[18]

Es un servidor de páginas web, siendo este un programa que permite acceder a páginas web alojadas en un equipo. Corre en una multitud de Sistemas Operativos, lo que lo hace prácticamente universal.

Entre sus principales características están:

- Es una tecnología gratuita de código fuente abierta, siendo esto lo que le da una transparencia a este software.
- Apache es un servidor altamente configurable de diseño modular.
- Trabaja con gran cantidad de Perl, PHP y otros lenguajes de script.
- Apache te permite personalizar la respuesta ante los posibles errores que se puedan dar en el servidor.
- Es muy configurable en la creación y gestión de logs. Apache permite la creación de ficheros de log a medida del administrador, permitiendo tener un mayor control sobre lo que sucede en él.

[17] berislav kucam.Detección de intrusiones con Snort: Técnicas avanzadas de IDS usando snort, Apache, MySQL, PHP, y ACID. disponible en: http://www.net-security.org/review.php?id=79 . 2 de mayo 2012

[18] Ciber aula Linux.una introducción a apache. Disponible en : http://linux.ciberaula.com/articulo/linux_apache_intro/ . 1 de mayo 2012

7.16. SNIFFER

Es un software que permite el análisis y monitoreo del tráfico de la red, a través de la captura de paquetes de información (tramas - frames).

Sus funciones principales son:

- Monitorear una red, para detectar y analizar fallos.
- Medir el trafico de la red, para determinar los horarios en que mayor se usan los recursos de la red en la organización.
- Detectar intrusos y nodos que carguen de tráfico a una red
- Para fines maliciosos como: robar contraseñas, interceptar mensajes del correo electrónico o espío de conversaciones.

8. METODOLOGÍA DEL PROYECTO

8.1. TIPO DE METODOLOGIA

Este proyecto tiene como tipo de investigación la exploratoria, ya que se estará haciendo referencia a un tema específico y casi desconocido ya que el conocimiento del tema es mínimo y se debe tratar con exactitud, se partirá de un tema de investigación donde se debe encontrar una falencia o un problema existente y así buscar y dar una solución tratando de profundizar en el tema para obtener mejor conocimiento sobre este.[19]

8.2. PROCESO

Se realiza el análisis de la infraestructura de red de la compañía y se encuentra que no poseen herramientas que ayuden a definir políticas de seguridad teniendo en cuenta que poseen equipos de protección frontal pero estas no ayudan a definir ni a localizar posibles falencias dentro de dicha infraestructura permitiendo que se realicen ataques desde internet hacia la compañía y ataques internos a los servidores o aplicaciones que prestan servicios, además no cuentan con un sistema de auditoria informática para el control y monitoreo de la red.

La implementación de un IDS(sistema de detección de intrusos) ayuda fortalecer los sistemas de seguridad y de control actuales definiendo políticas que protejan las diferentes redes que se tienen al interior de la compañía, así se encuentra que la combinación de un conjunto de herramientas creadas para facilitar las tareas de monitoreo puede ser implementada como solución a esta necesidad, entre las herramientas analizadas se tienen SNORT que actúa como analizador de trafico de red, llevando toda la información a logs del sistema o guardándolos en bases de datos estructuradas para lograr su integración, además de un conjunto de reglas que contienen patrones de detección de anomalías dentro de las comunicaciones., detección de eventos a nivel de los protocolos de red que facilitan la detección de intrusos y posibles amenazas al interior de la red.

[19] Frank morales .tipos de investigación. Disponible en : http://manuelgross.bligoo.com/conozca-3-tipos-de-investigacion-descriptiva-exploratoria-y-explicativa . 1 de mayo 2012

Otra de las herramientas que hacen parte de este proyecto es la integración de base de datos en MySQL las cuales guardaran la información que es arrojada por SNORT y procesada por el lenguaje PHP para facilitar la creación de informes que serán publicados por medio de un servidor web con los controles necesarios para que esta información solo sea vista por personal autorizado dentro de la compañía, todo este conjunto de herramientas debe ser cuidadosamente configurado de tal forma que permita una implementación limpia para así evitar que información no importante se mezcle provocando errores en la definición de políticas o toma de decisiones.

9. CRONOGRAMA DE TRABAJO

Para el cronograma de trabajo se realizó un plan que describe los avances del proyecto por semanas hasta su presentación final.

CRONOGRAMA DE ACTIVIDADES																
ACTIVIDADES	**SEMANAS**															
	S1	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**S9**	**S10**	**S11**	**S12**	**S13**	**S14**	**S15**	**S16**
FASE I																
FASE II																
FASE III																
FASE IV																
FASE V																
FASE VI																
FASE VII																

Tabla 1. Cronograma de Actividades

- **Etapa I:** Elaboración de la propuesta del proyecto a implementar. Con base en aplicaciones e implementaciones de seguridad empresariales se proponen diferentes ideas que pueden servir como proyecto y deben ser escogidas por la universidad como un proyecto valido

- **Etapa II:** Gestión de permisos de ingreso y horario de trabajo. Una vez aprobado el proyecto se pedirán los permisos necesarios para el ingreso y utilización de los equipos disponibles para el proyecto**.**

- **Etapa III:** Recolección de información necesaria para determinar viabilidad en la implementación. De acuerdo a la información obtenida y los recursos que posee la compañía se procederá con el análisis de requerimientos y la adquisición de hardware para las respectivas pruebas.

- **Etapa IV:** Implementación e instalación de servicios, En esta etapa se realizara el montaje de pruebas necesarias para llevar a cabo los objetivos propuestos.

- **Etapa V:** Pruebas de funcionamiento, En esta etapa se realizara una serie de pruebas que confirmen que el sistema propuesto funciona y puede ser llevado a producción.

- **Etapa VI:** Puesta en producción. Una vez se configure, se pruebe y se afinen los detalles se pasara a producción, etapa en la cual el sistema estará estable y debe cumplir con los objetivos para los cuales fue diseñado e implementado.

- **Etapa VII:** Exposición ante jurados. Etapa final de aprobación por parte de los jurados de la universidad donde aprobaran el proyecto.

10. DESARROLLO DEL PROYECTO

10.1. ANTECEDENTES

La red de datos de la compañía Tennis S.A. cuenta con una infraestructura de red que brinda a sus usuarios servicios a las distintas aplicaciones de la compañía, estos servicios se encuentran en servidores de aplicaciones, que ofrecen también navegación web, recursos compartidos, etc. Todo estos sistemas están interconectados por redes físicas e inalámbricas con la ayuda de dispositivos como router's y switch's, repartidos por las diferentes áreas de la compañía, facilitando así a los usuarios el desplazamiento por cualquier departamento interno, además se posee una Lan to Lan que interconecta los puntos de venta servicio que se tiene con un proveedor de servicios de internet y con el cual se tiene un contrato para prestar este servicio y el de internet, dentro de todos los sistemas de protección que se tienen existe la presencia de firewall que protegen el ingreso a los servidores y limitan el acceso de los usuarios a ciertas redes y servicios, lo mismo pasa con los visitantes que están limitados a ciertas áreas pero con más restricciones, en la actualidad la compañía no cuenta con un sistema de monitoreo que informe o alerte sobre anomalías en el comportamiento normal de la red, en la detección de bugs, que puedan ser explotados por personas inescrupulosas que deseen hacer cualquier tipo de daño ya sea por investigar, venganza de empleados descontentos, curiosidad o superación personal de personas expertas en temas de seguridad, etc.

Esquema Inicial

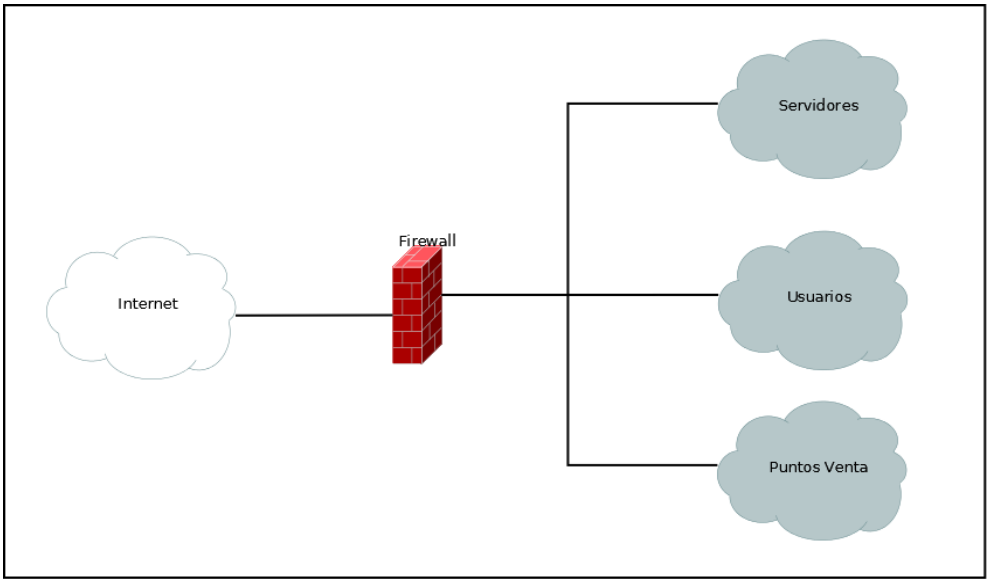


Figura 6. Esquema inicial

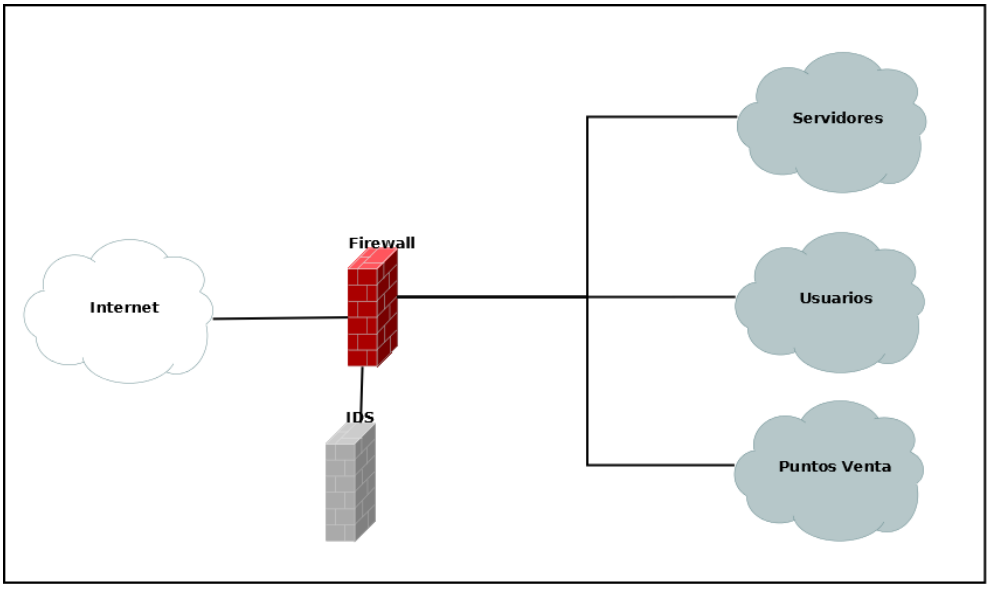


Figura 7. Esquema propuesto

10.2. IMPLEMENTACION

Para la implementación del proyecto se procede a utilizar herramientas de software libre como parte de la viabilidad técnica y económica, dentro del software utilizado cabe mencionar que para el funcionamiento del sistema de detección de intrusos se hace necesaria la integración de varias aplicaciones en las cuales se encuentran la Base de datos mysql, el lenguaje de programación PHP, El servidor de páginas web Apache, y el sistema de detección de intrusos que se ha seleccionado es Snort. Todas estas herramientas en conjunto forman un sistema de detección de intrusos con el cual se pueden generar reportes que pueden ser analizados de forma más amigable y cómoda por parte del encargado de la seguridad o del monitoreo de la red.

10.2.1. Instalación sistema Operativo GNU/Linux Debian:

Se realiza el download del ISO de la página principal de la distribución GNU/Linux Debian para continuar con su respectiva instalación, como la instalación se realizara en ambientes de producción y este se enfocara en la seguridad y estabilidad del servicio y de la maquina se recomienda bajar la versión STABLE de 64b del sistema operativo[20], una vez se baja el ISO del sistema debe ser quemado en un CD-ROM para su respectiva instalación.

[20]Debían.org. instalación de sistema operativo .disponible en : http://cdimage.debian.org/debian-cd/6.0.5/amd64/iso-cd/debian-6.0.5-amd64-netinst.iso . 30 de abril 2012

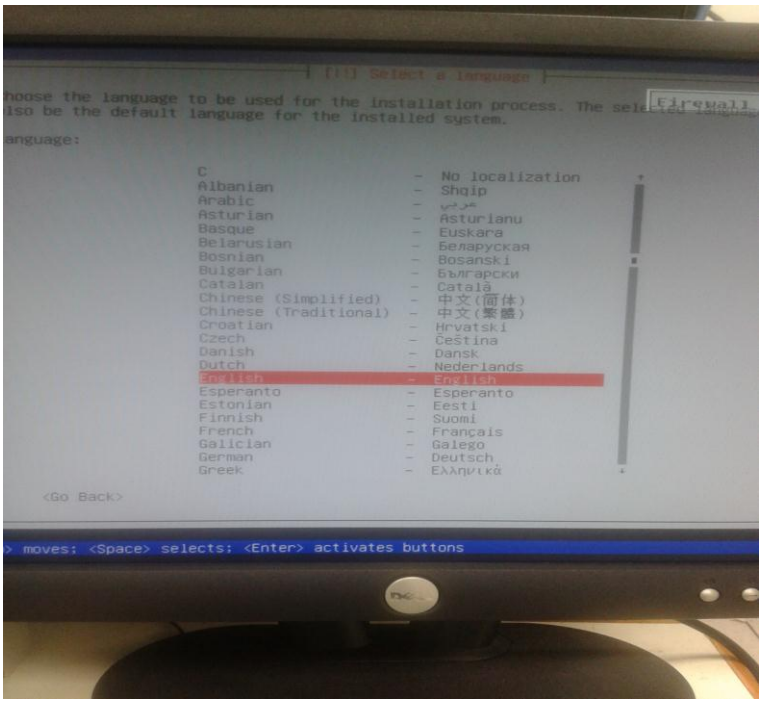


Figura 8. Idioma por defecto del sistema operativo.

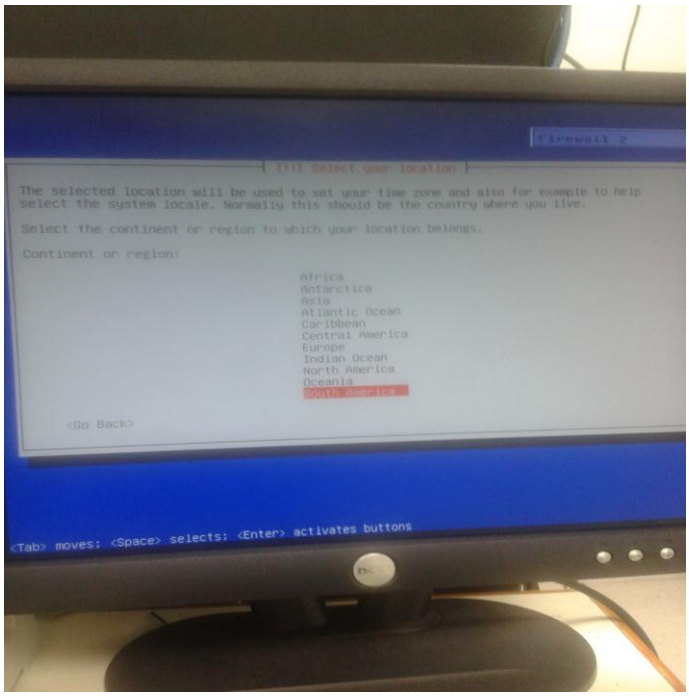


Figura 9. Selección del continente y ubicación geográfica.

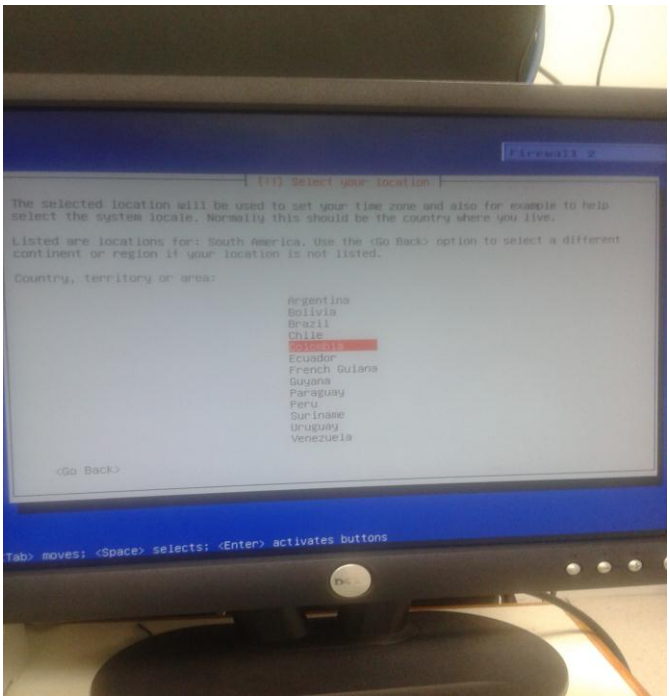


Figura 10. Selección del país.

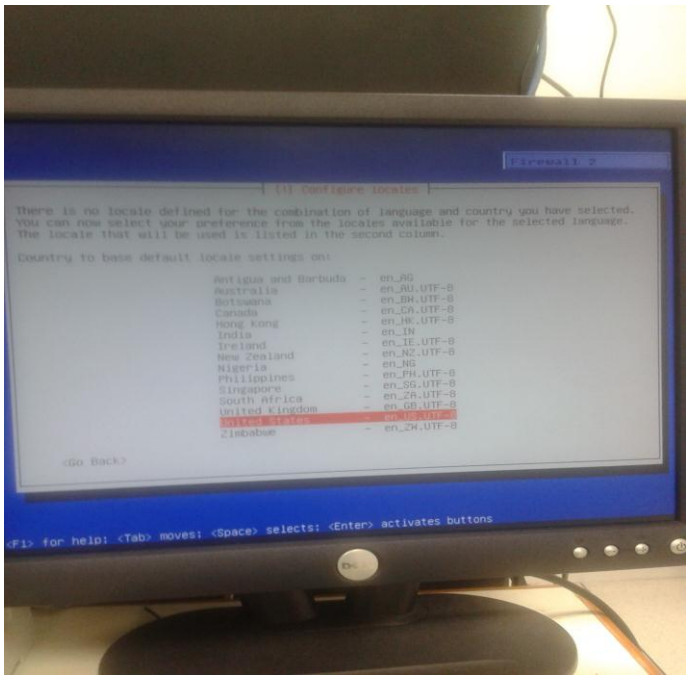


Figura 11. Configuración de idiomas soportados por el sistema.

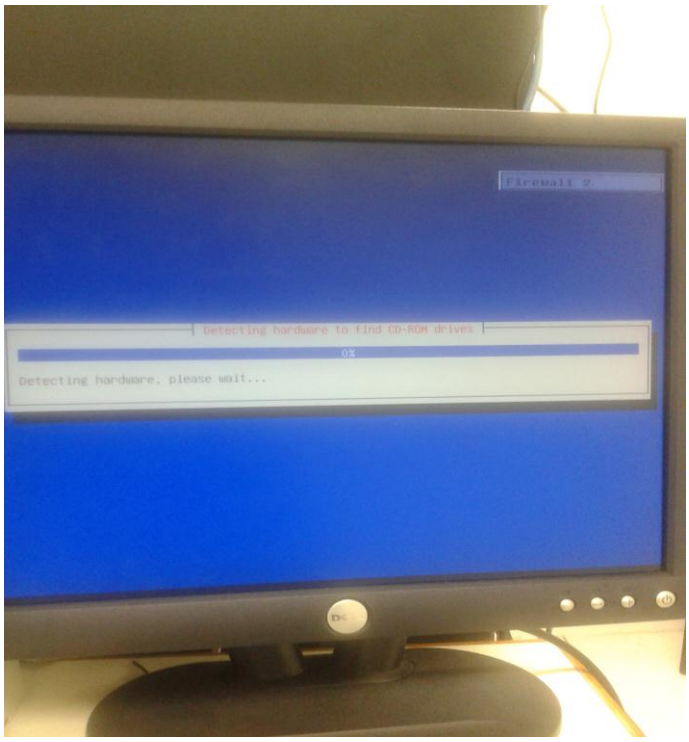


Figura 12. Detección de hardware.

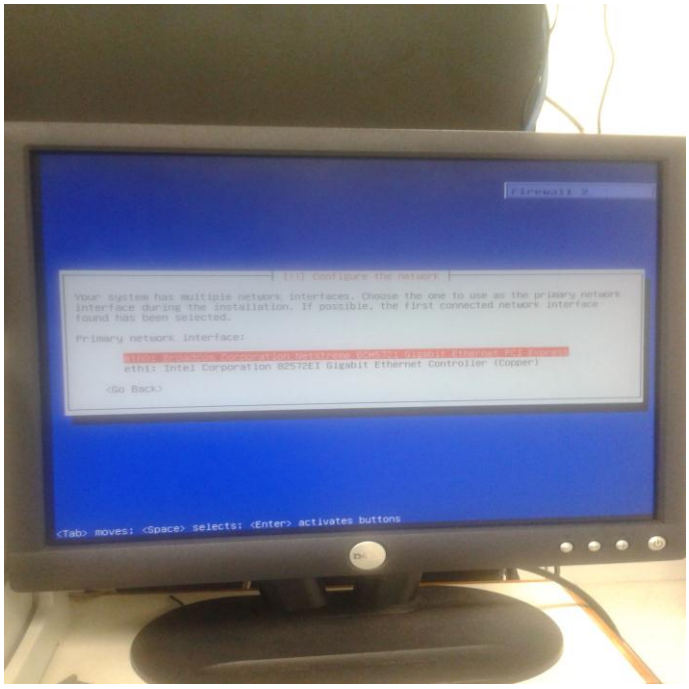


Figura 13. Configuración de la red.

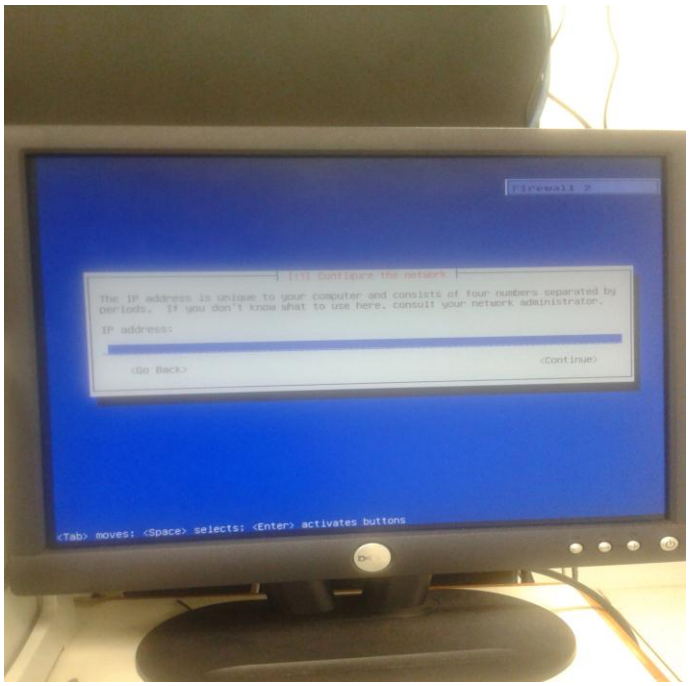


Figura 14. Particionamiento del disco.

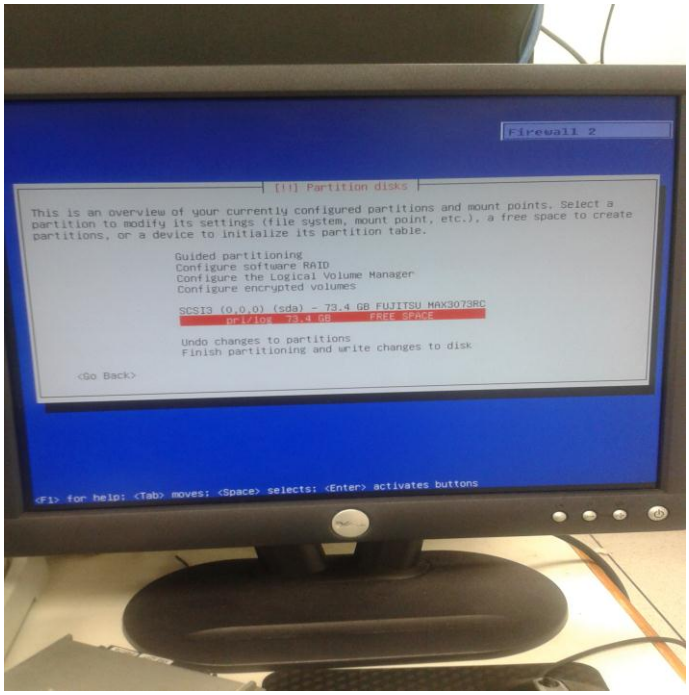


Figura 15. Menú particionamiento de disco

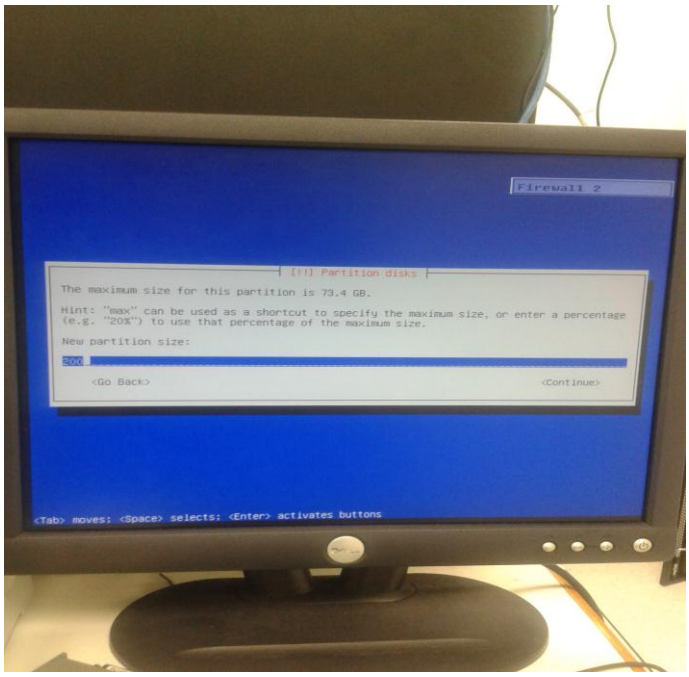


Figura 16. Tamaño de la partición en Gigas Megas o Kilobytes.

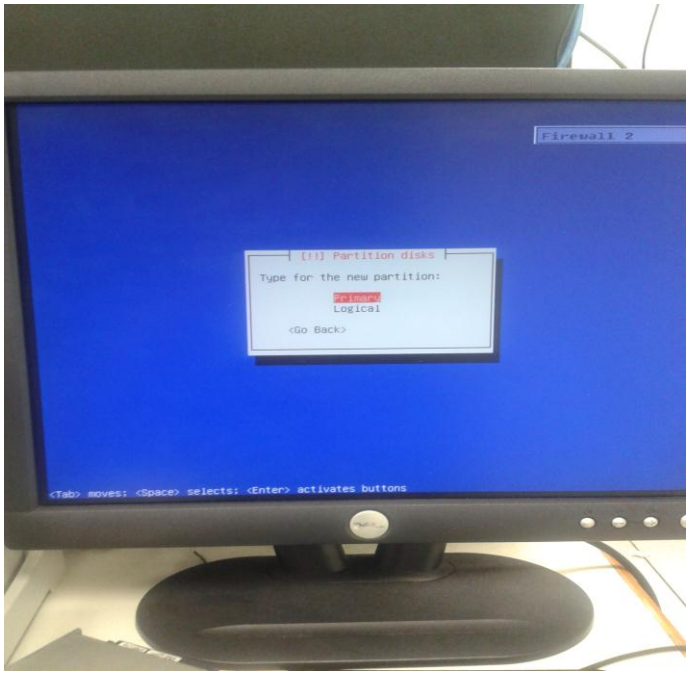


Figura 17. Selección del tipo de partición Primaria/lógica.

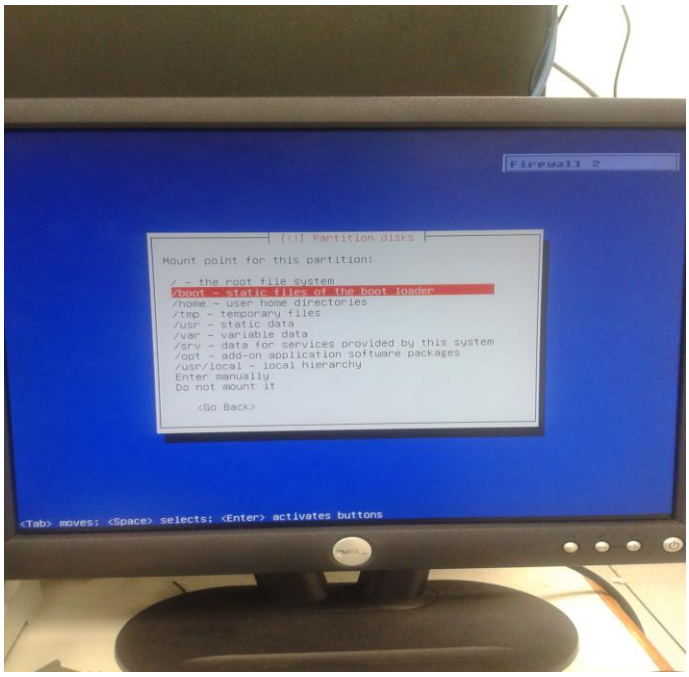


Figura 18. Elección del punto de montaje del particionamiento.

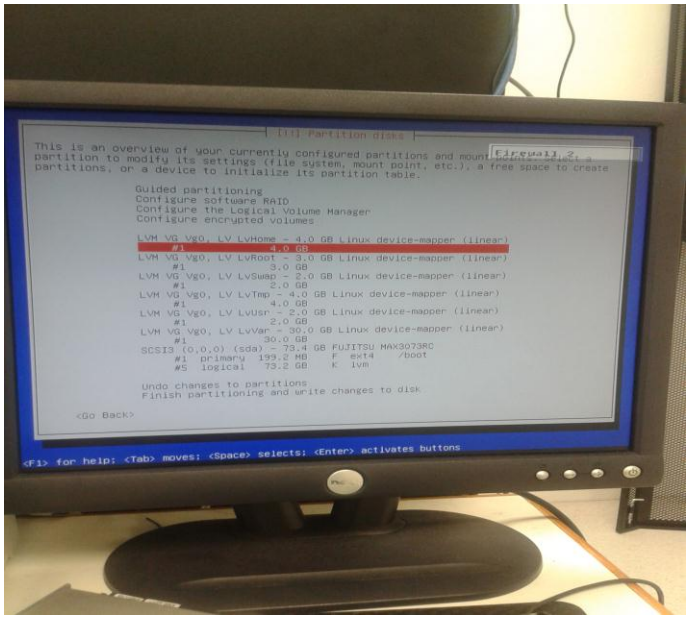


Figura 19. Finalización del particionamiento, el sistema en esta fase muestra las particiones creadas.

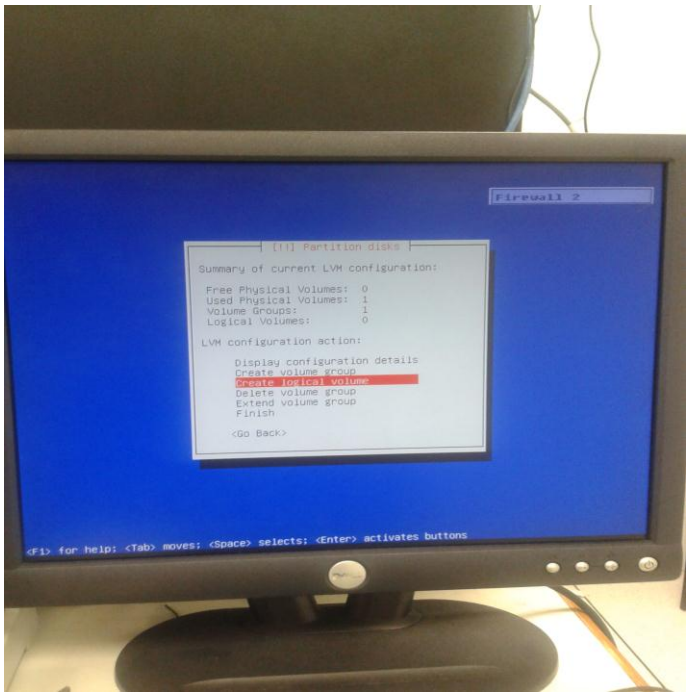


Figura 20. Creación de un volumen lógico.

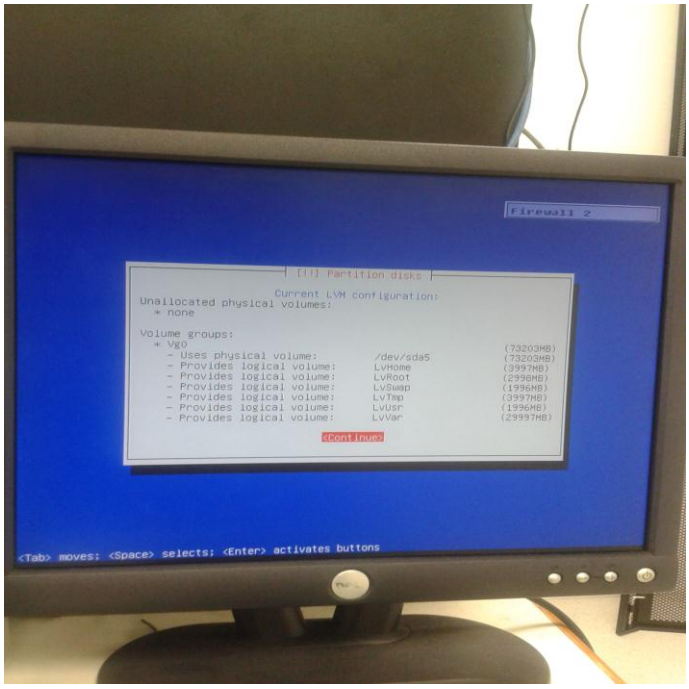


Figura 21. Listado de los volúmenes lógicos.

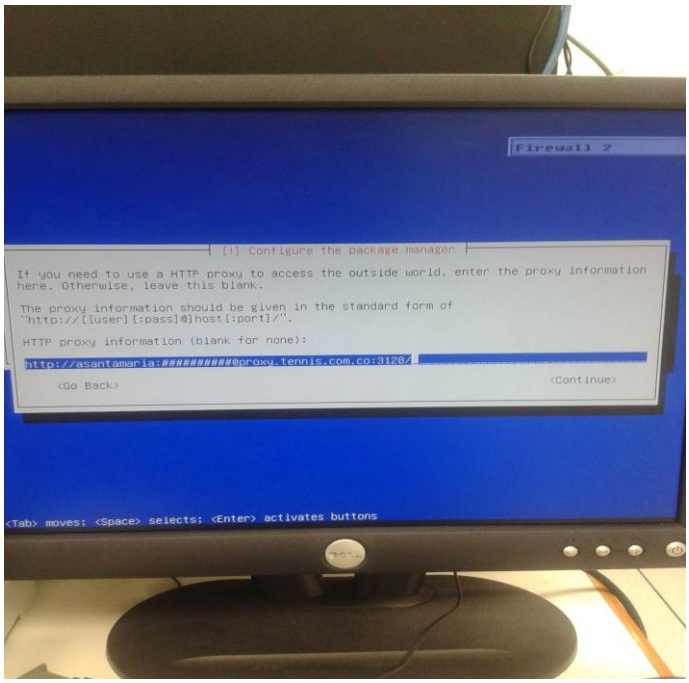


Figura 22. Configuración del proxy para la actualización de la paquetería, este proceso es importante ya que dependiendo de cómo este comunicado a internet puede actualizar el sistema.

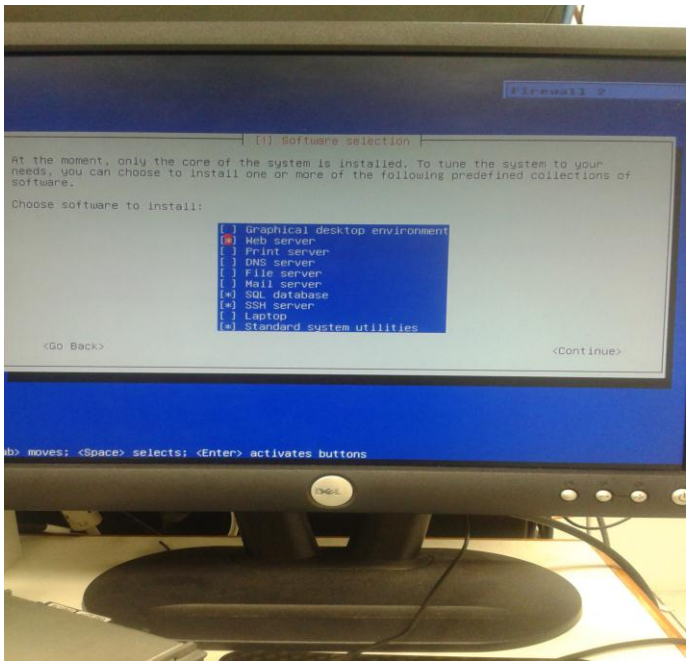


Figura 23. Instalación de paquetería estándar, estas opciones deben ser seleccionadas teniendo en cuenta las funciones que va a cumplir el servidor.

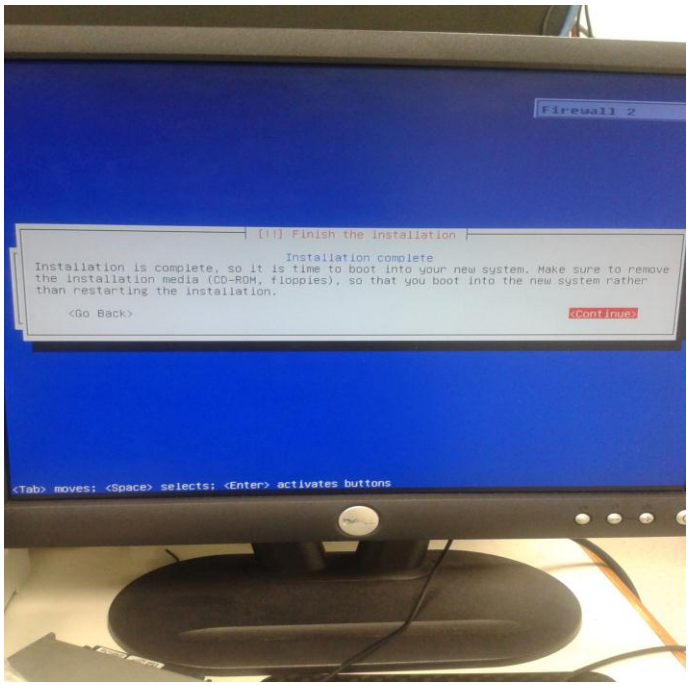


Figura 24. Finalización de la instalación y reinicio del servidor.

Figura 25. El servidor iniciando luego de la instalación.

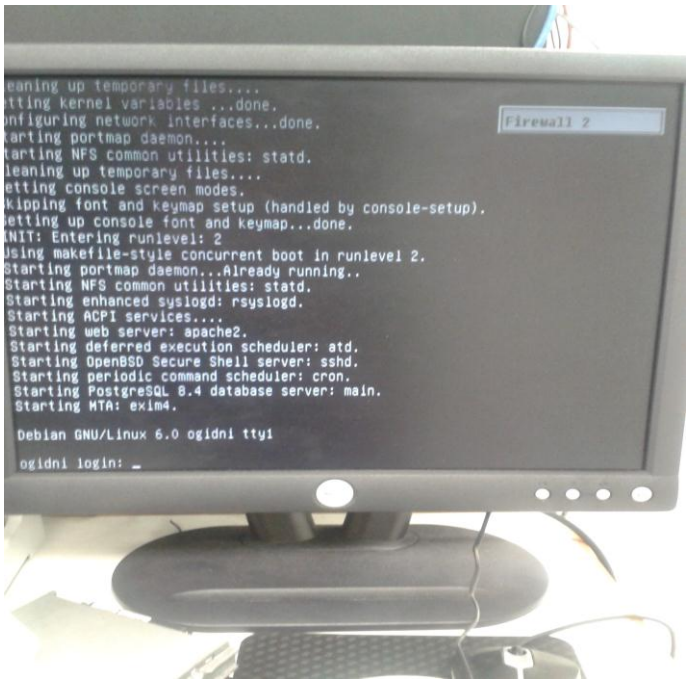


Figura 26. Inicio de sesión de usuario o login del sistema una vez se da por finalizada la instalación.

10.2.2. Interfaces de red: Una vez instalado el sistema operativo base se procederá a la configuración de las interfaces de red que permitirá que el sistema de detección de intrusos funcione adecuadamente (Por razones de seguridad y confidencialidad de la compañía los datos reales no serán publicados):

- Se hace necesario que se configuren 3 interfaces de red con las siguientes especificaciones:
    - Interfaz para acceso a Internet
    - Interfaz para acceso a L2L
    - Interfaz para acceso a LAN(VLAN)

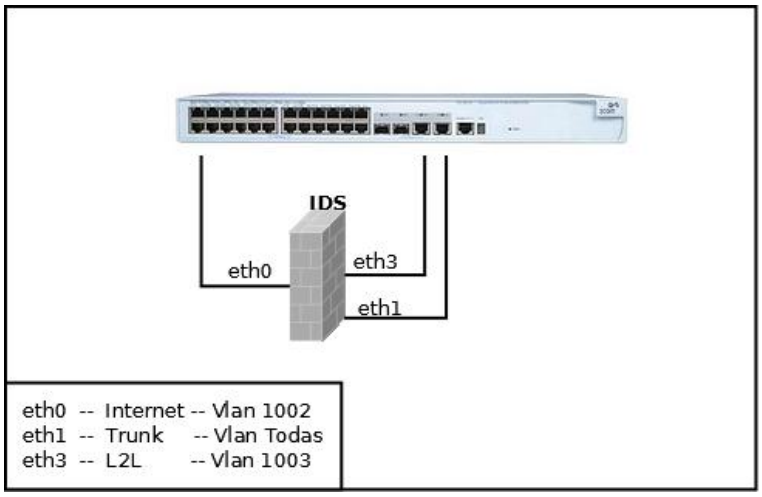


Figura 27. Interfaces de red necesarias para la implementación

Para la configuración de las interfaces de red se debe tener en cuenta que estas van a soportar VLAN's para lo cual se debe instalar el paquete que contiene el protocolo 802.1Q.

Se debe instalar el paquete llamado VLAN para poder realizar la configuración de las VLAN's

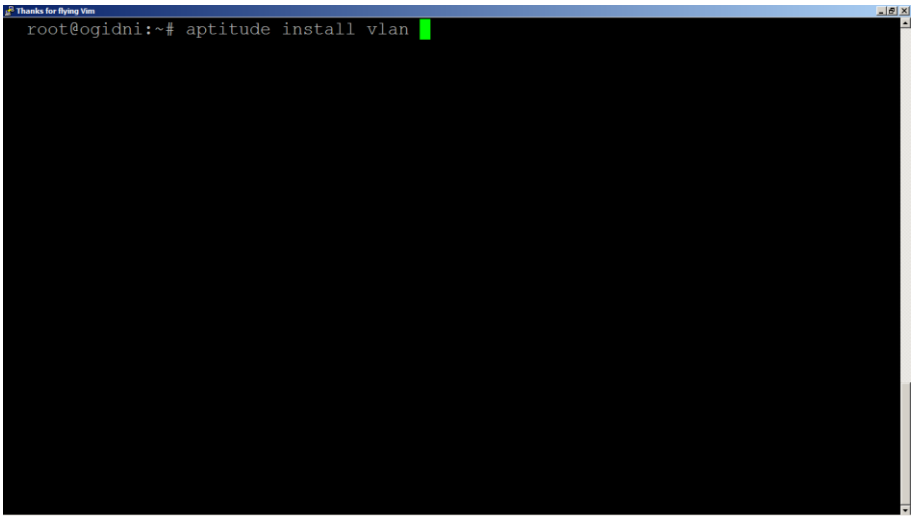


Figura 28. Instalacion del paquete vlan

Se debe editar el archivo de configuración de las tarjetas de red con el fin de asignar el direccionamiento IP de acuerdo a las necesidades del proyecto

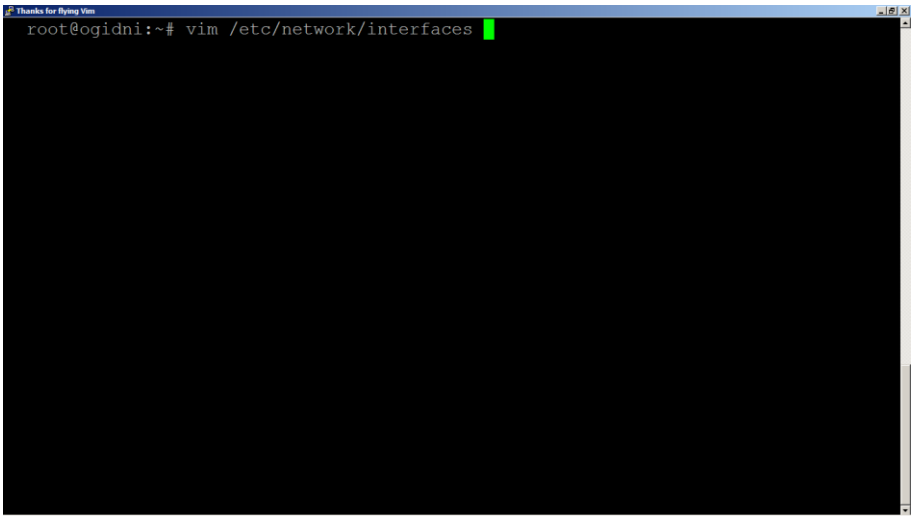


Figura 29. Archivo Configuracion de interfaces

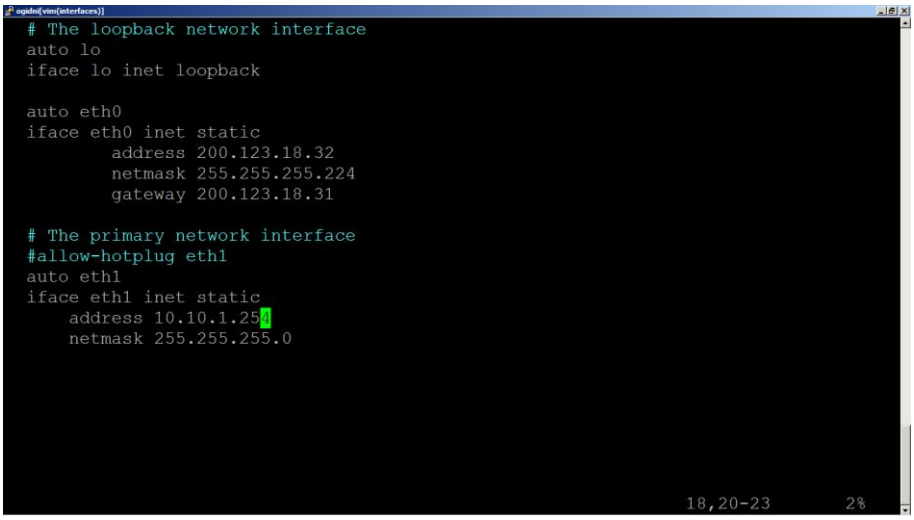


Figura 30. Contenido configuracion Interfaces fisicas de red

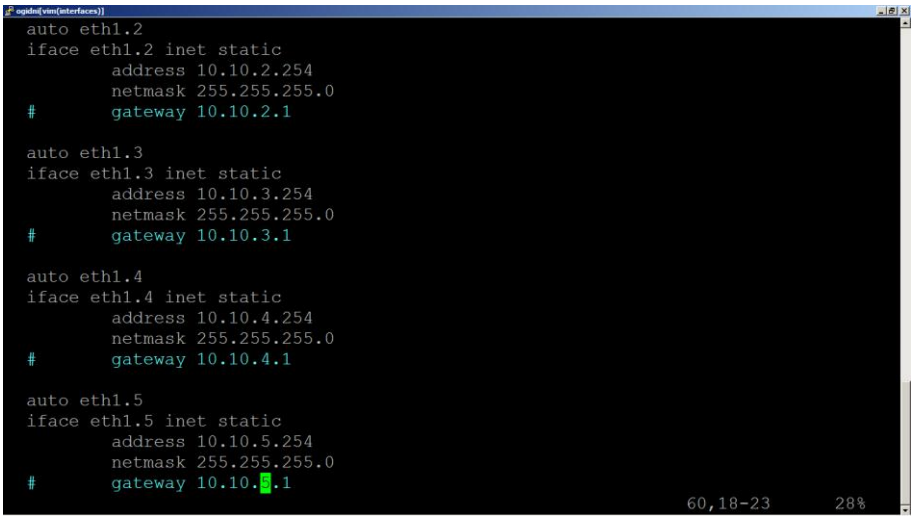


Figura 31. Contenido configuraciones interfaces virtuales de red

Se debe instalar el paquete vlan para activar el soporte en el sistema operativo una vez realizada la instalación del paquete se debe modificar el sistema operativo con el fin de que el kernel cargue el modulo del protocolo 802.1Q en el archivo /etc/modules y adicional la línea correspondiente a al protocolo:

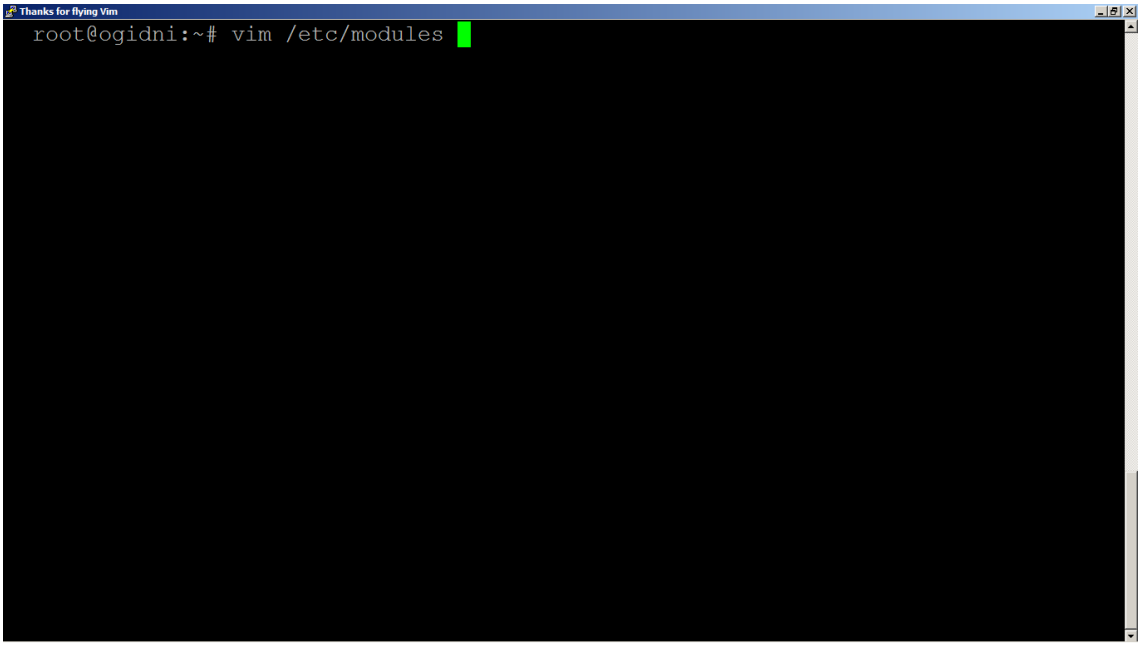


Figura 32. Archivo de carga de modulos del kernel

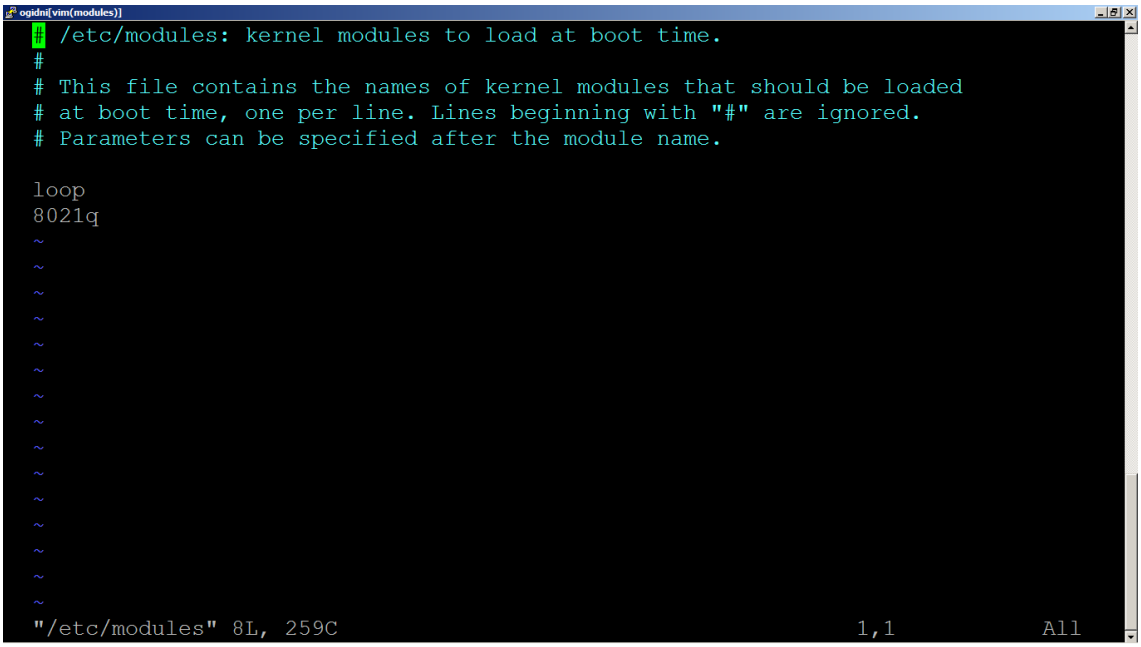


Figura 33. Contenido Configuración de módulos para activa soporte de VLAN's

10.2.3. Procedimiento para la implementación de SNORT

- El software a utilizar debe seguir el siguiente esquema:

El sistema base debe estar soportado por el sistema operativo GNU/Linux, en el tema de la seguridad interviene Shorewall que es implementado para facilitar la creación de reglas en Iptables este software tiene la particularidad de que la creación de reglas se hace a través de la consola y realiza las tareas de una forma más modular, El sistema de detección de intrusos utilizado es SNORT y actúa como Sniffer de red, este arroja la información a archivos de texto llamados logs y utiliza también la base de datos en MySQL para almacenar información que es parte crucial en la creación y generación de reportes con ACID y que son generados con el lenguaje PHP que accede a consultar esta información a dichas bases de datos y son publicados por un servidor web que para este caso se utilizó Apache y que publica la información recolectada en informes que pueden ser graficados estos informes pueden ser vistos y administrados desde un navegador por el administrador del sistemas o por personal de monitoreo asignado por la compañía.

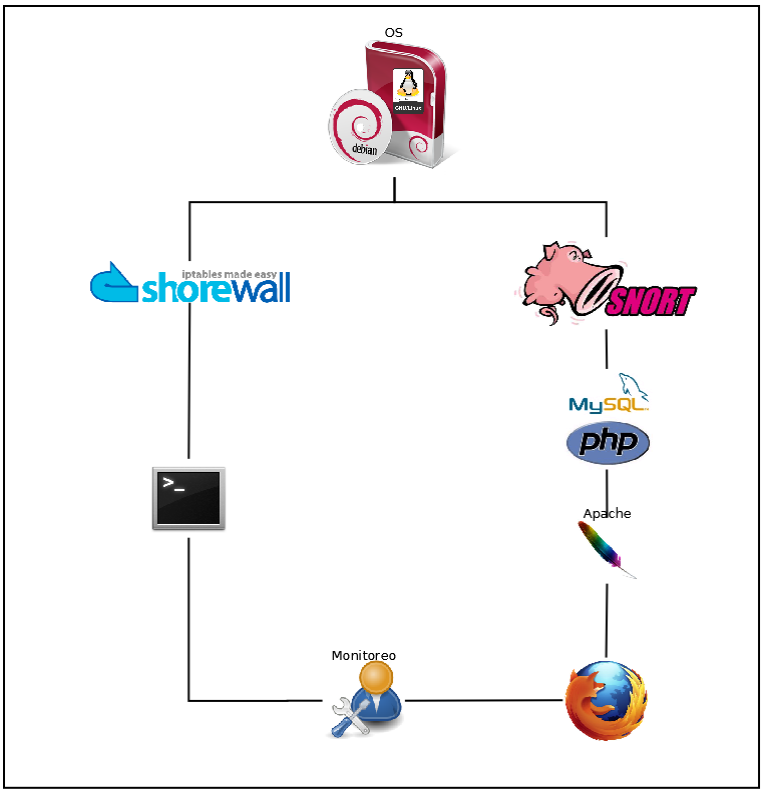


Figura 34. Esquema de aplicación.

10.2.4. Instalación y configuración de MySQL: Se debe instalar la última versión del motor de la base de datos soportada por la distribución de Linux, en este caso se utilizara MySQL como motor de base de datos

Figura 35. Instalación paquete mysql-server

Se definir una contraseña para el administrador de la base de datos que en este caso se llama “**root”.**

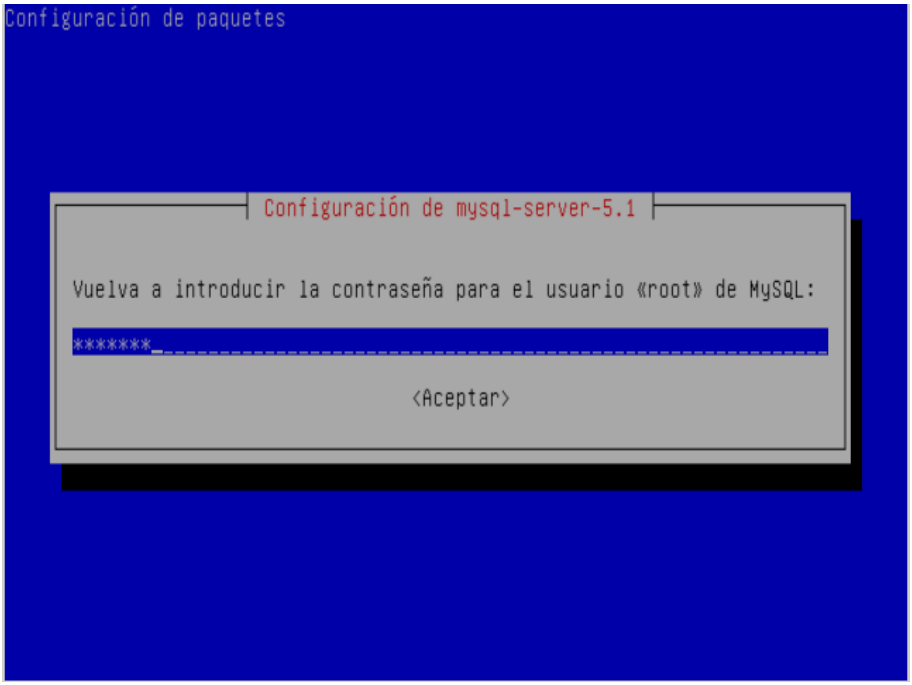


Figura 36. Password Usuario administrador MySQL

10.2.5. Instalación y configuración PHP: El lenguaje por defecto para el procesamiento de información y elaboración de informes es PHP, el cual debe estar instalado y configurado de forma que se integre con el servidor web “Apache”

Figura 37. Instalación paquete PHP

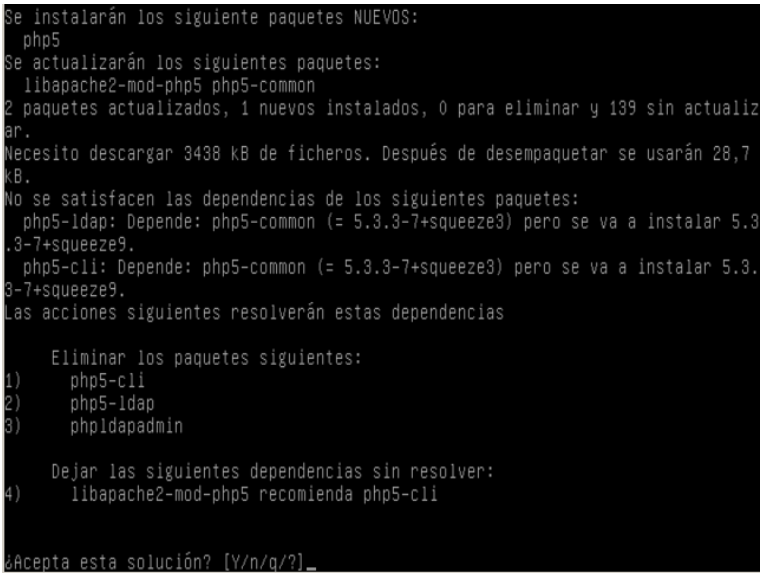


Figura 38. Pantalla para aceptar cambios en la paquetería del sistema.

10.2.6. Instalación y configuración de SNORT: Una vez instalado el motor de la base de datos se debe crear un usuario y su respectiva base de datos que soporte la información que “Snort” arrojara y quedara almacenada, para esto se debe crear un usuario y una contraseña y así mismo asignar los permisos al usuario para poder manipular los datos.

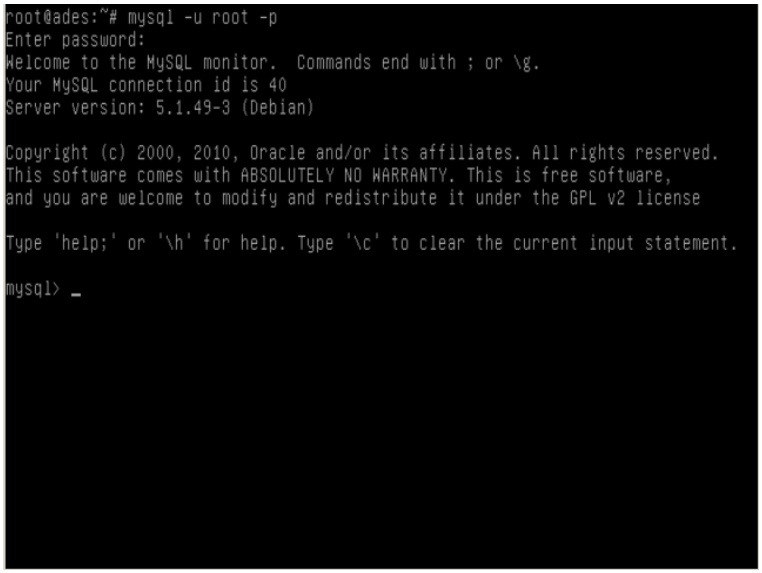


Figura 39. Ingreso como administrador al motor de base de datos

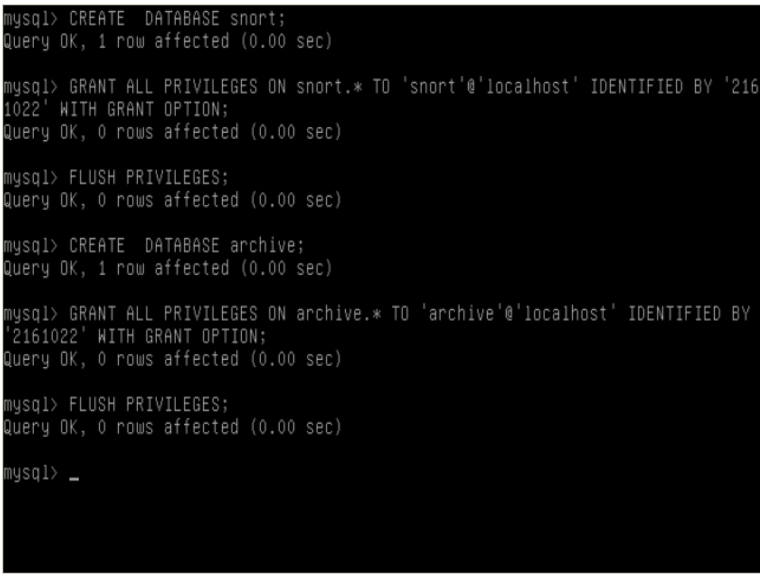


Figura 40. Creación de usuarios, base de datos y permisos en MySQL

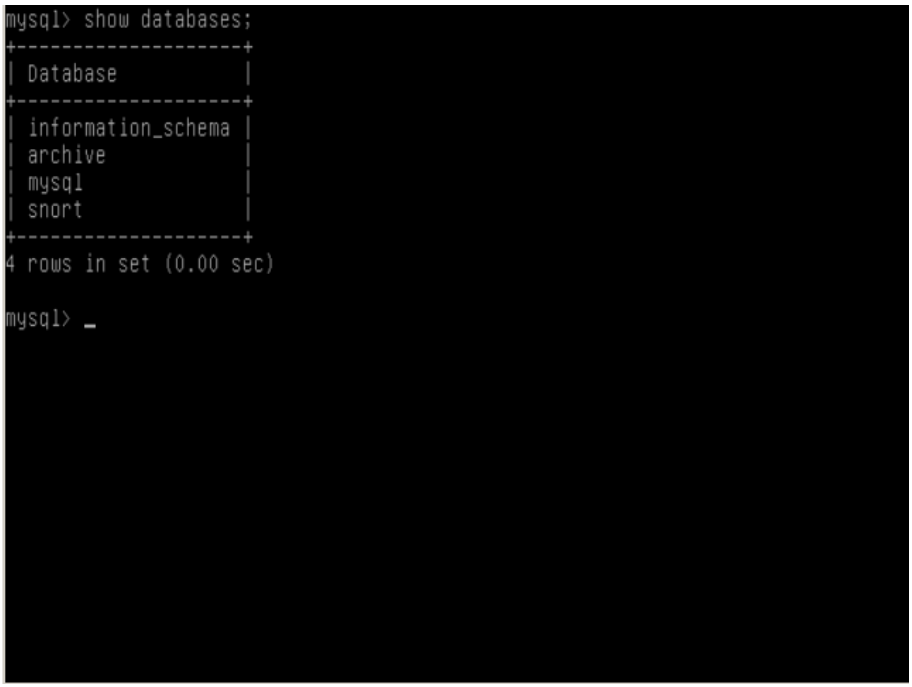


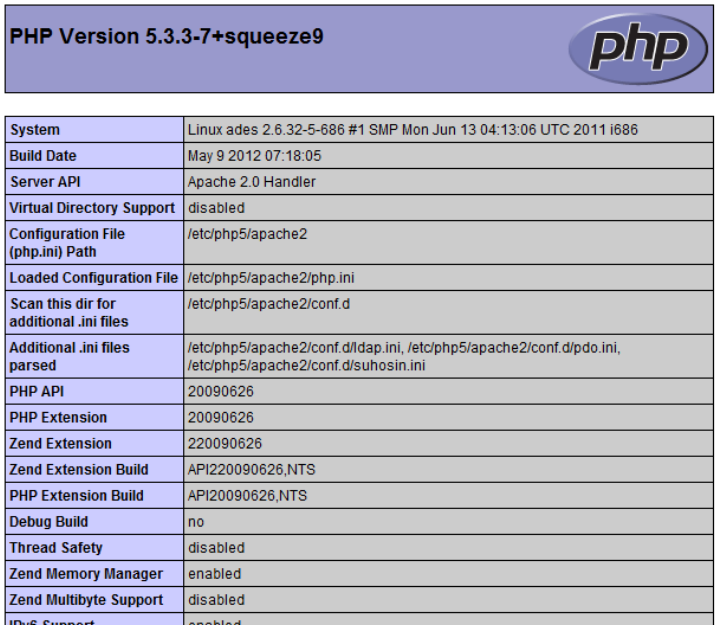
Figura 41. Bases de datos creadas

Figura 42. Importando la estructura de la base de datos

10.2.7. Configuración del servidor web Apache: Se debe realizar la prueba de que tanto el lenguaje de programación como el servidor web están funcionando correctamente, para esto se crea un archivo de test para probar el lenguaje Php y se debe acceder a los resultados por medio del navegador web con la dirección local(localhost)

Figura 43. Archivo de test para Php.

Figura 44. Edición del archivo con sentencias en PHP.



PHP Version 5.3.3-7+squeeze9

System	Linux ades 2.6.32-5-686 #1 SMP Mon Jun 13 04:13:06 UTC 2011 i686
Build Date	May 9 2012 07:18:05
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/ldap.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/suhosin.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,NTS
PHP Extension Build	API20090626,NTS
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled

Figura 45. Página web que muestra los parámetros del test de PHP

Se habilita la extensión de módulos dinámicos utilizados por el generador de reportes ACID

```
; Dynamic Extensions ;
;;;;;;;;;;;;;;;;;;;;;

; If you wish to have an extension loaded automatically, use the following
; syntax:
;
;   extension=modulename.extension
;
; For example, on Windows:
;
;   extension=msql.dll
;
; ... or under UNIX:
;
;   extension=msql.so
;
; ... or with a path:
;
;   extension=/path/to/extension/msql.so
;
; If you only provide the name of the extension, PHP will look for it in its
; default extension directory.
extension=mysql.so
extension=gd.so
                                                              943,1         50%
```

Figura 46.Cambios en la configuración deL ARCHIVO php.ini

Se debe reiniciar el servicio para que los cambios surtan efecto sobre el servidor web

Figura 47. Reinicio del servidor web apache.

Configuraciones adicionales y no menos importantes necesarias para que el resto de los programas funcionen correctamente y que actúan como dependencias de algunas funciones dentro de la integración del IDS

Figura 48. Paquetería necesaria para la integración de las herramientas

10.2.8. Instalación y Configuración ACID: Este software es una interfaz web desarrollada en PHP que muestra los registros que son almacenados por Snort en una base de datos o en un simple archivo de log, debe estar como requisito y previamente instalado y funcionando la integración del servidor web Apache y el lenguaje de programación Php.

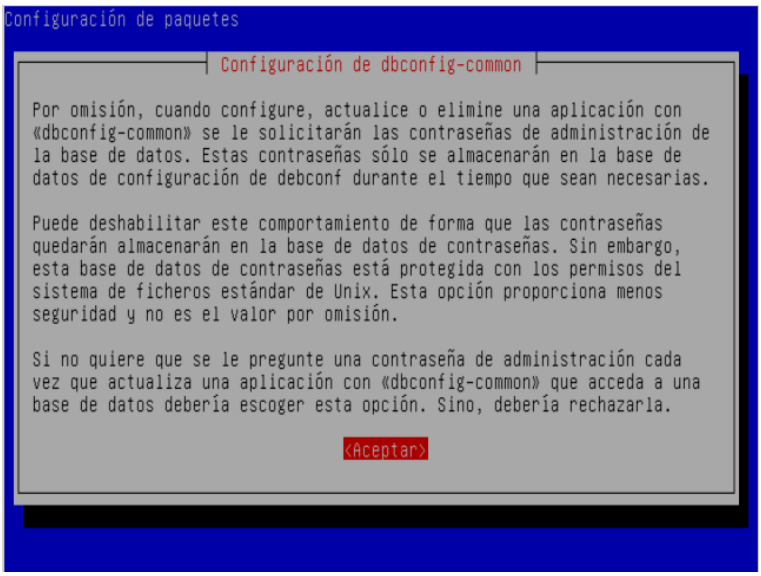


Figura 49. Instalación paquete Acid

Como se mencionó anteriormente Acid debe acceder a la base de datos donde Snort guarda la información de todo lo que pasa por las interfaces de red.

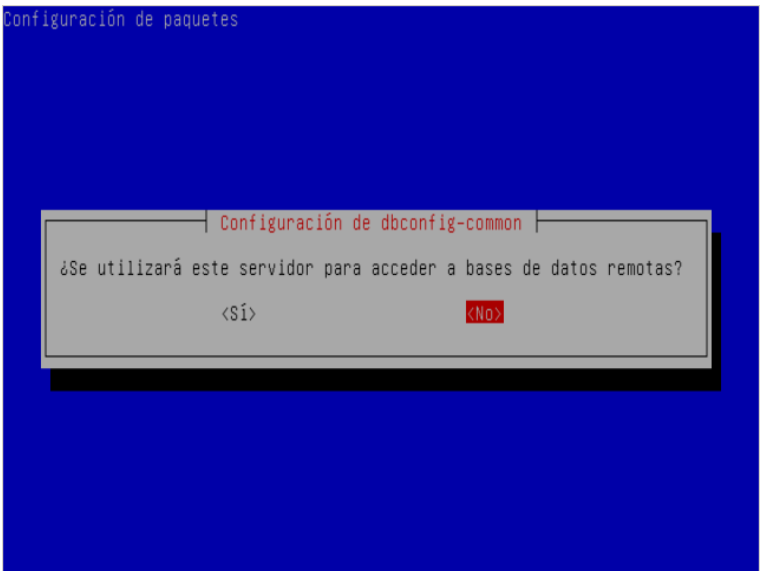


Figura 50. Permisos para el acceso a base de datos remotas

Además de necesitar el servidor web Apache para su funcionamiento

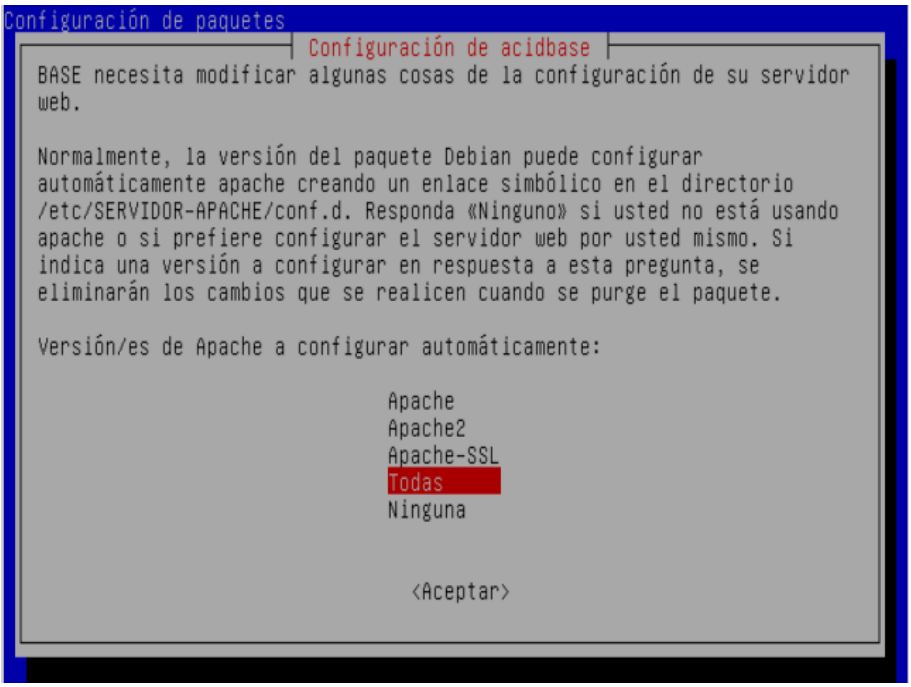


Figura 51. Configuración de parámetros en el servidor web apache

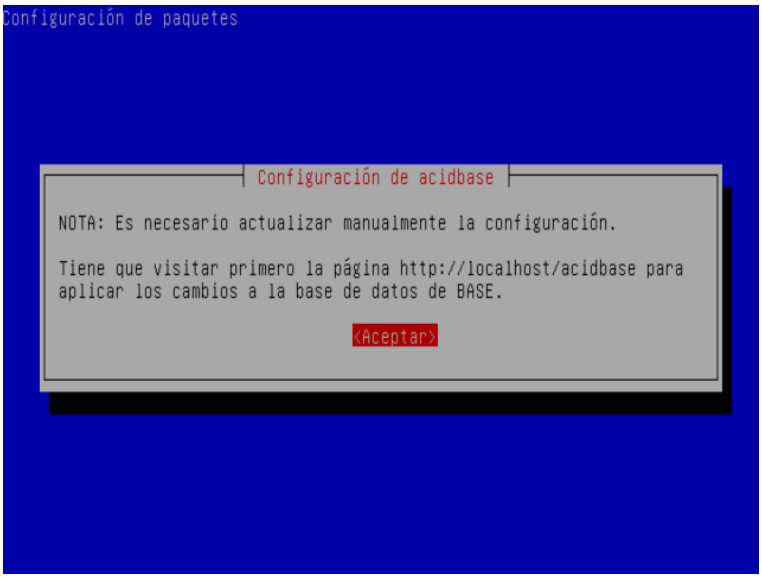


Figura 52. Información acerca de cómo ingresar a la configuración de la aplicación

Acid soporta diferentes motores de base de datos, dentro de estos se encuentran MySQL y PostgreSQL pero para el caso del proyecto se utilizara MySQL.

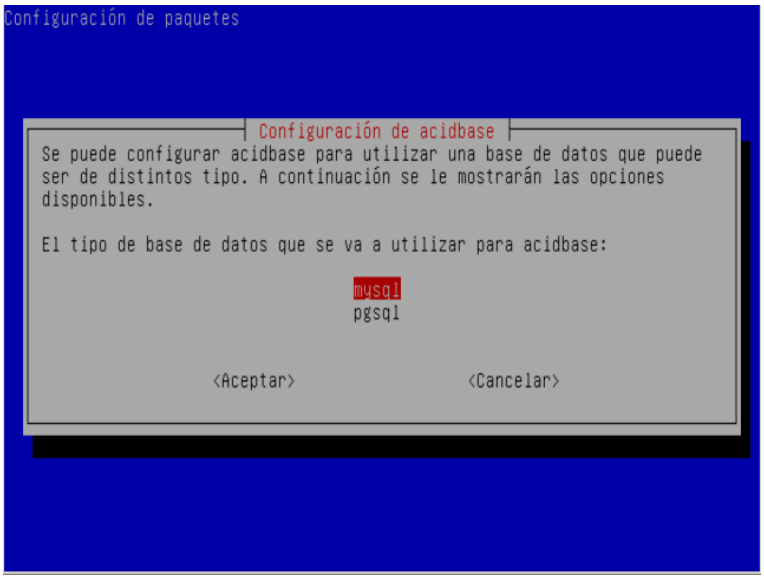


Figura 53. Elección del motor de base de datos

El acceso a la base de datos se debe hacer por un puerto de red que por defecto MySQL maneja el 3306.

Figura 54. Elección del método de conexión a la base de datos

Por seguridad, en la configuración del motor de base de datos MySQL, se debe tener en cuenta que si comparte recursos con una aplicación se le debe dar acceso a los usuarios solo de manera local

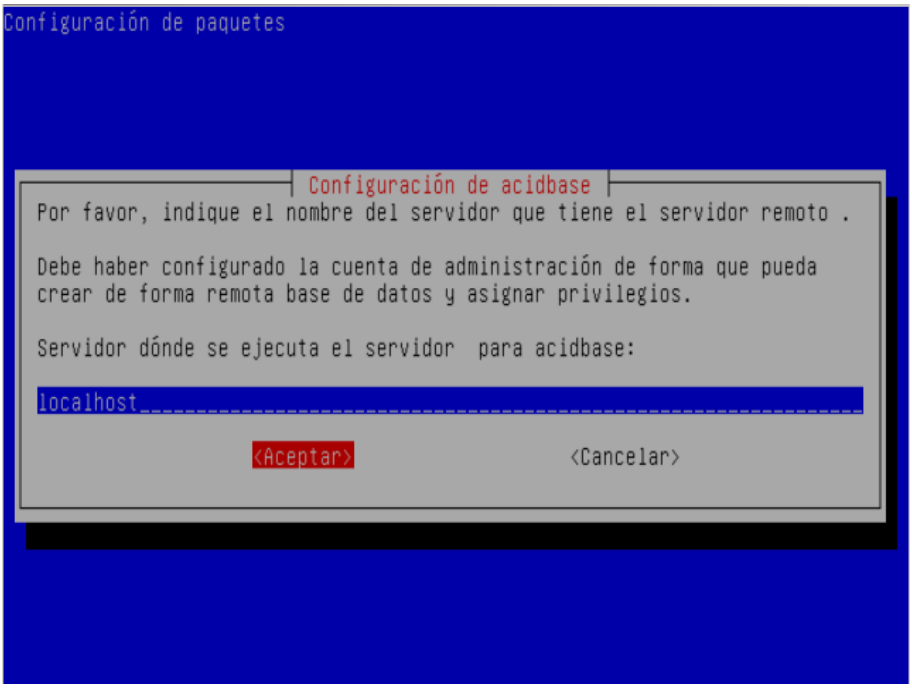


Figura 55. Servidor donde se ejecuta el motor de base de datos

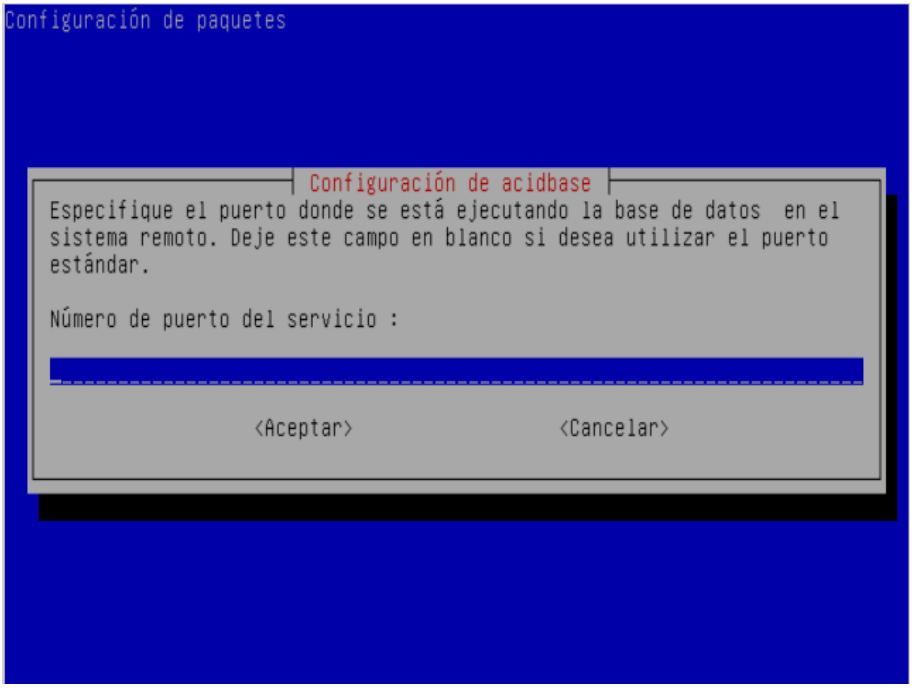


Figura 56. Puerto de conexión TCP

Se ingresa información que fue anteriormente configurada en el motor de la base de datos.

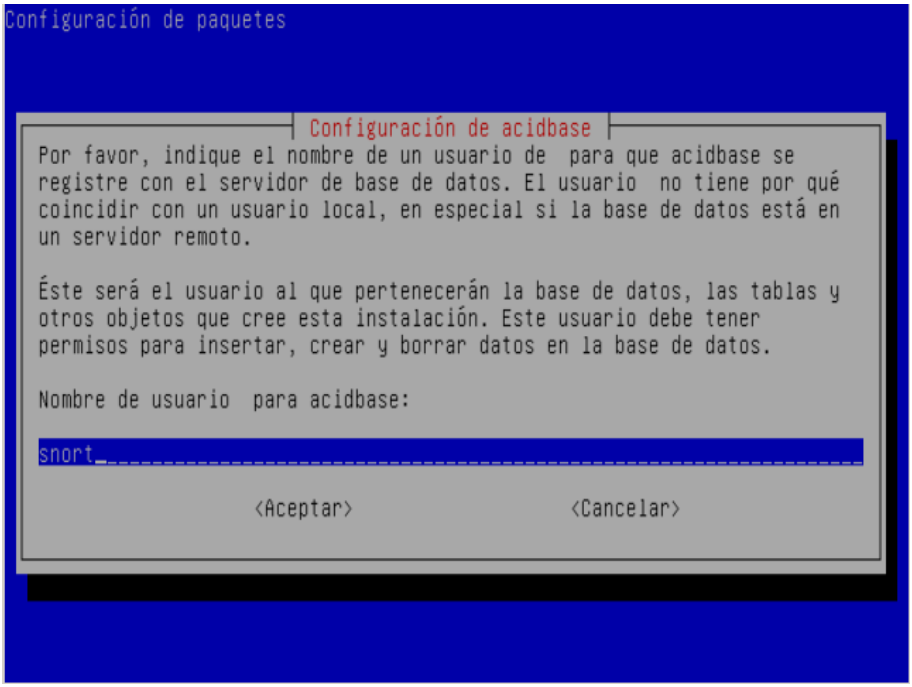


Figura 57. Usuario de conexión a la base de datos

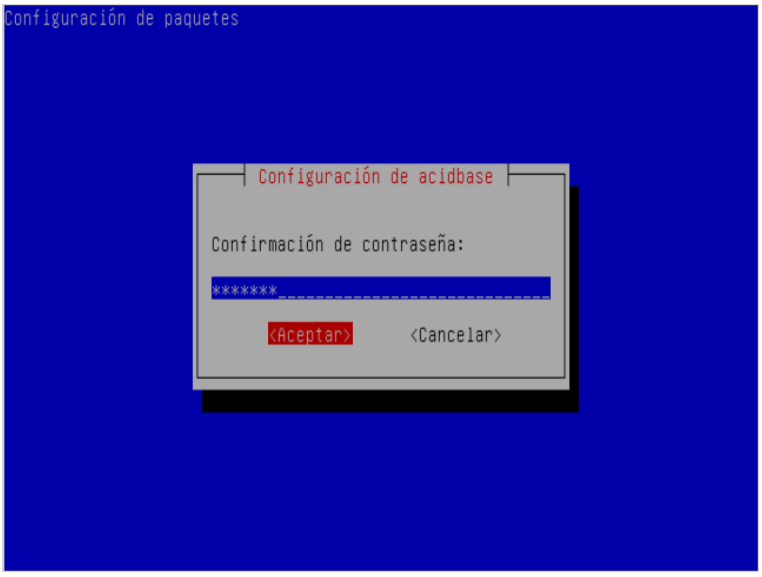


Figura 58. Contraseña del usuario de conexión a la base de datos

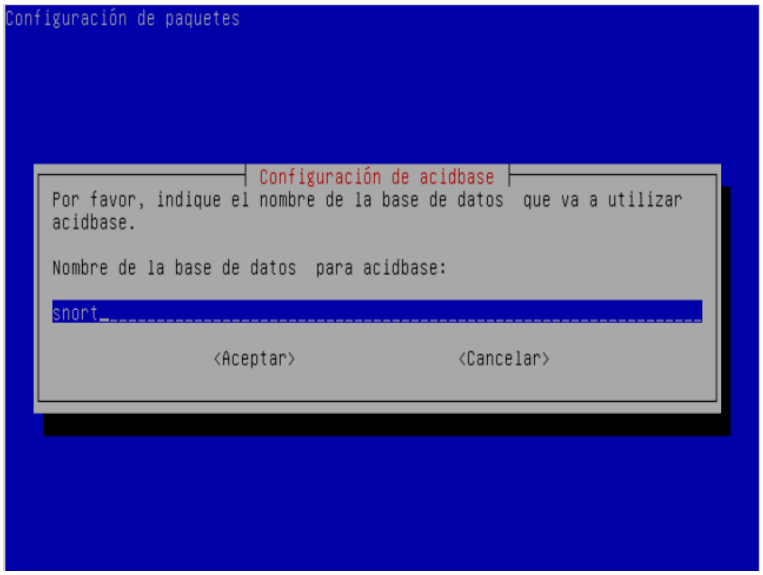


Figura 59. Nombre de la base de datos configurada

Por seguridad en el servidor web Apache se debe configurar el ingreso a la aplicación web a la(o las) maquinas autorizadas para el monitoreo y se debe editar el archivo de configuración del directorio de la aplicación

Figura 60. Archivo de configuración Acid/Apache

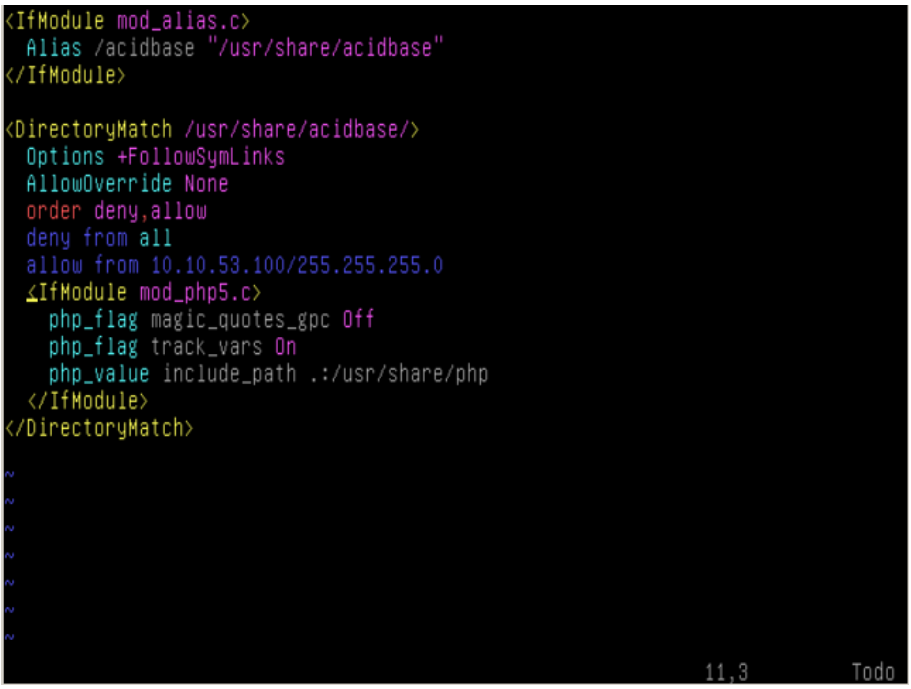


Figura 61. Contenido del archivo de configuración

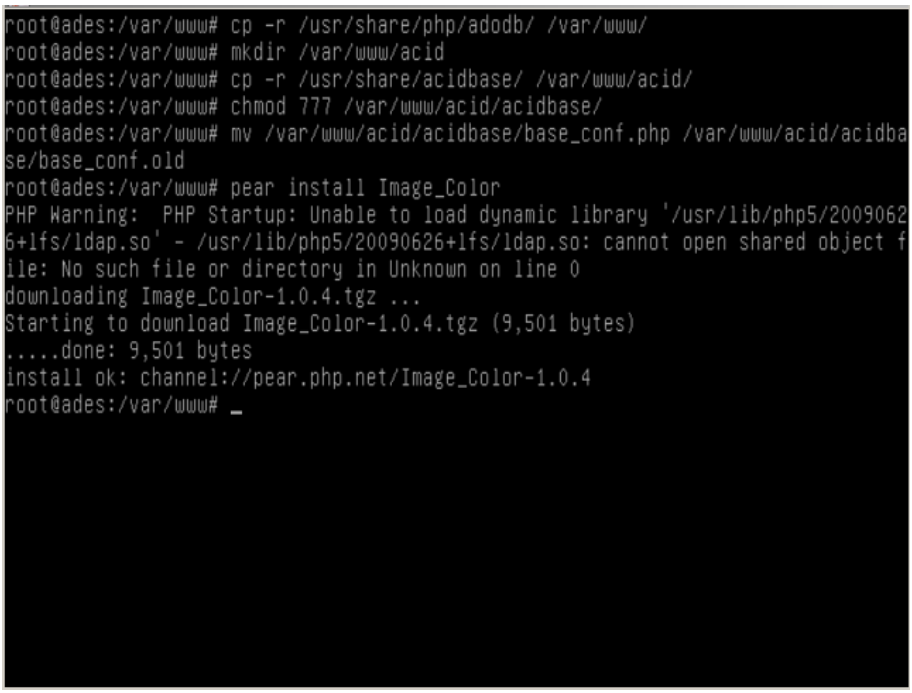


Figura 62. Copia de archivos que serán expuestos por el servidor web

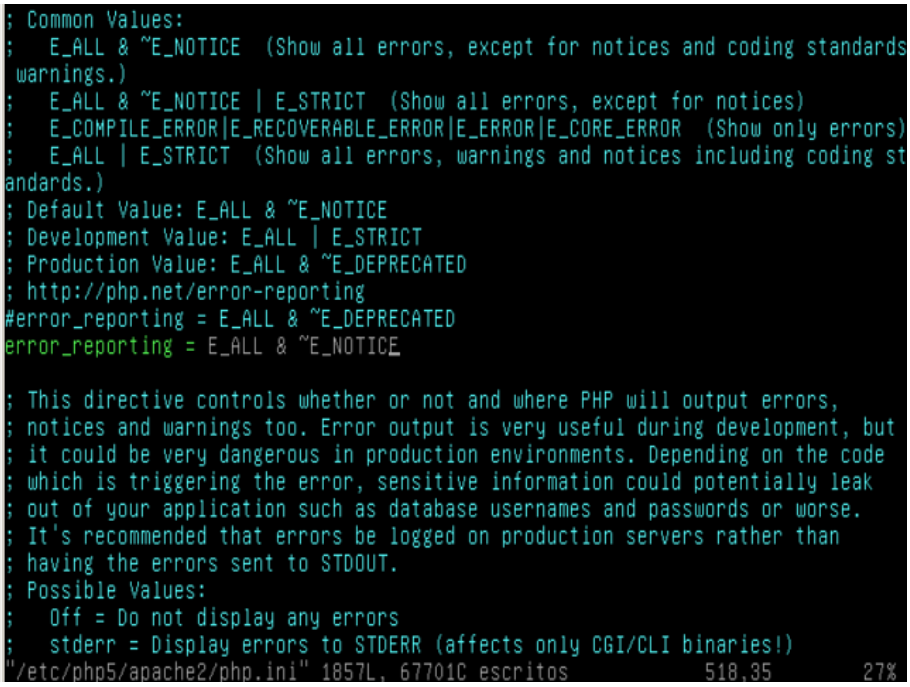


Figura 63. Cambios en el archivo php.ini para activar los reportes de error

10.2.9. Configuración ACID: Una vez instalado el ACID, se debe ingresar a la página web donde se configura el resto de la aplicación las imágenes a continuación demuestran el proceso por el cual se realiza dicha configuración, se debe tener a mano la información de la (las) bases de datos creadas como: usuario, contraseña, rutas de archivos.

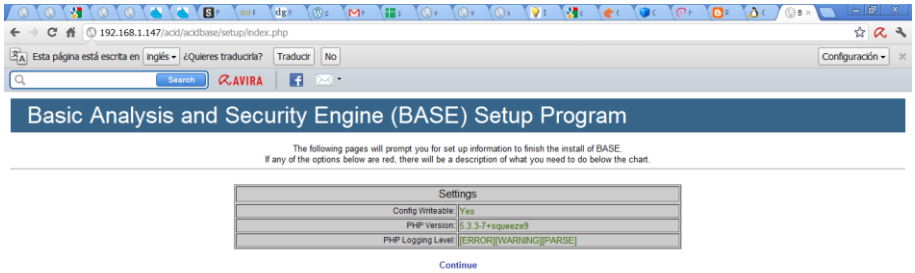


Figura 64. Configuración web del analizador de reportes

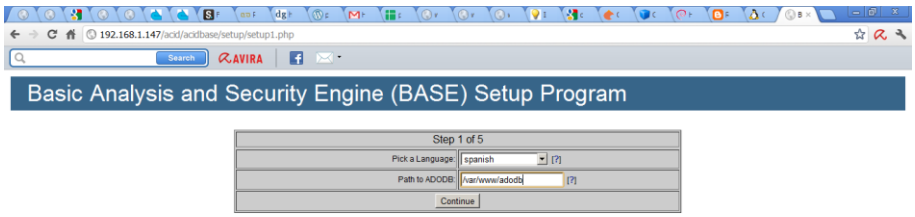


Figura 65. Elección del idioma del analizador de reportes

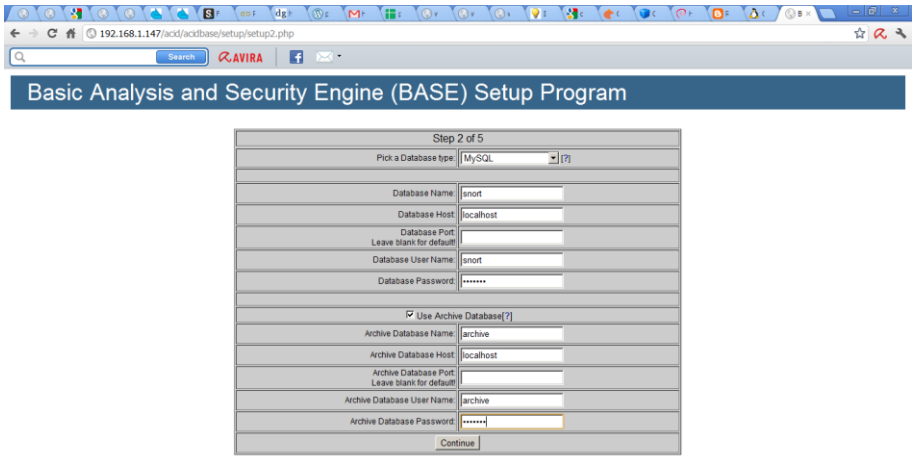


Figura 66. Datos de conexión para la base de datos

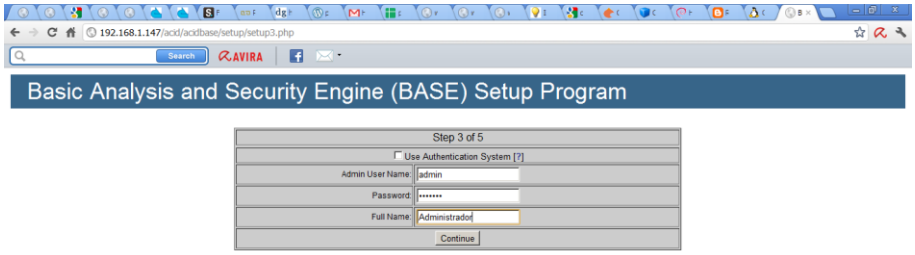


Figura 67. Elección del usuario administrador de los reportes

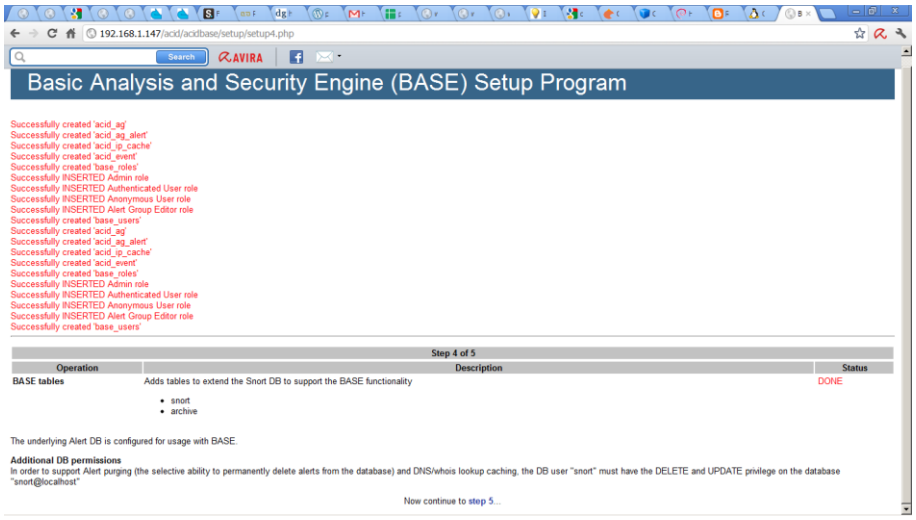


Figura 68. El sistema informa que el proceso de configuración fue satisfactorio

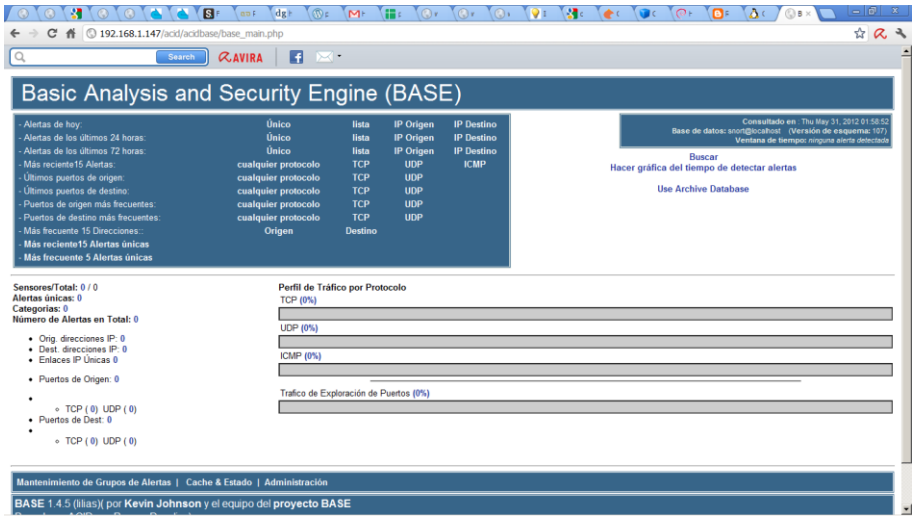


Figura 69. Interfaz web para la generación de reportes

11. PRESUPUESTO

Equipos	Cantidad	Valor Unidad	Total
Servidor	1	3700000	3’700.000
Tarjeta de red PCI-X	1	270000	270.000
Cables de red certificados	3	30000	90.000
		Total	4’060.000

Tabla 2. Presupuesto de equipos

Mano de obra	Cantidad (horas)	Valor Hora	Total
Análisis de la infraestructura de red	12	30000	360.000
Configuración firewall	1	700000	1’200.000
Instalación sistema (IDS)	1	750000	750.000
		Total	2’260.000

Tabla 3. Presupuesto de mano de obra

Valor Implementación	Total
Equipos	4’060.000
Mano de obra	2’260.000
Total	6’320.000

Tabla 4. Presupuesto de implementación

12. CONCLUSIONES

La protección de las redes de datos es una tarea compleja debido al incremento de nuevas técnicas que ayudan a los intrusos a explotar vulnerabilidades y a aprovechar descuidos del personal de seguridad, esta misma razón afecta al software que cada vez es más complejo debido a su implementación en nuevas tecnologías que necesitan tanto de otro software como de hardware especial, así mismo se puede hablar de la implementación de protocolos de red, por esta razón herramientas como SNORT que ayudan a la detección de intrusos no se pueden dejar de lado ya que brindan una ayuda muy importante a los administradores de la seguridad de los sistemas o al personal de monitoreo de las compañías a encontrar más fácilmente vulnerabilidades y a establecer políticas más drásticas en las redes de datos.

Este proyecto propone a SNORT como herramienta para la detección de intrusos en redes de computadores de fácil implementación y configuración utilizando reglas de filtrado que ayudan a ubicar los paquetes que viajan por esta, rastreando máquinas y servicios, ataques a servidores y ataques de denegación de servicios, SNORT se convierte así en una solución de bajo costo y de fácil implementación que puede ser utilizada en cualquier parte de la red dependiendo de las zonas que deseen analizar y que ayudará a fortalecer la seguridad a través de patrones o comportamientos sospechosos que pueden comprometer la integridad de la información.

La instalación y configuración de un IDS (Sistema de detección de Intrusos) proporciona mayor seguridad y tranquilidad a los sistemas informáticos ofreciendo un mayor control del tráfico que pasa por las redes de datos minimizando los riesgos de seguridad y de vulnerabilidades que se puedan presentar.

13. BIBLIOGRAFIA

- Debían.org. Guía de instalación de Debian GNU/Linux. Disponible en: http: //www.debian.org/releases/stable/amd64/ .9 de abril 2012
- Debían.org. Guía de instalación de Debian GNU/Linux. Disponible en: http: //www.debian.org/releases/stable/amd64/ .9 de abril 2012
- Mayra Pazmiño; Jorge Aviles; cristina abad. Captura y análisis de los ataques informáticos que sufren las redes de datos de la ESPOL, implantando una honeynet con miras a mejorar la seguridad informática en redes de datos del Ecuador. Disponible en: https://www.dspace.espol.edu.ec/bitstream/123456789/4203/1/6722.pdf. 9 de abril 2012
- Matt Curtin. Introduction to network security. Disponible en: http: //www.interhack.net/pubs/network-security/. 20 de abril 2012
- DAVID FERNANDEZ VAAMONDE .detección de intrusos en GNU/Unix. Disponible en : http://stuff.gpul.org/2003_jornadas/doc/deteccion_de_intrusos/deteccion_de_intrusos.html . 5 de marzo 2012
- Linux party group.El Sistema de Detección de Intrusos: Snort. (Windows y Linux).Disponible en: http: //www.linux-party.com/modules.php?name=News&file=article&sid=6000.16 de abril 2012
- PELLO XABIER ALTADILL IZURA. iptables manual practico. Disponible en: http: //www.pello.info/filez/firewall/iptables.html#2. 5 de marzo 2012
- OPENBSD.traduccion de direcciones de red NAT. Disponible en: http: //www.openbsd.org/faq/pf/es/nat.html .10 de marzo 2012
- UNAM CERT. Firewall personales. Disponible en: http: //www.seguridad.unam.mx/descarga.dsc?arch=422. 1 de mayo 2012
- el prisma. cortafuegos-firewall. Disponible en: http: //www.elprisma.com/apuntes/ingenieria_de_sistemas/cortafuegos/default3.asp. 1 de abril de 2012
- PELLO XABIER ALTADILL IZURA. iptables manual práctico. Disponible en: http: //www.pello.info/filez/firewall/iptables.html#2. 5 de marzo 2012
- wilmer haumani corboba. instalar firewall en Linux server con shorewall. Disponible en: http: //configurarlinuxserver.com/instalarfirewallenlinuxserver.pdf . 6 de marzo 2012
- juanjoalvarez.net .configuración absurdamente rápida del firewall shorewall. Disponible en:http://juanjoalvarez.net/es/detail/2009/jun/25/configuracion-absurdamente-rapida-del-firewall-sho/ .8 de marzo 2012
- PIERPAOLO PALAZZOLI, MATTEO VALENZA. utilizando snort inline. Disponible en: http: //snortattack.org/docs./SNORT_ES.pdf. 5 de marzo 2012

- cesar Gonzales. snort+mysql+acid: sistema de detección de intrusos open source. Disponible en:http: //linuca.org/body.phtml?nIdNoticia=13 . 10 de marzo 2012
- DANIEL PECOS .PostGreSQL vs. MySQL .disponible en: http: //danielpecos.com/docs/mysql_postgres/index.html .1 de mayo 2012
- berislav kucam.Detección de intrusiones con Snort: Técnicas avanzadas de IDS usando snort, Apache, MySQL, PHP, y ACID. Disponible en: http: //www.netsecurity.org/review.php?id=79 . 2 de mayo 2012
- Ciber aula Linux.una introducción a apache. Disponible en: http://linux.ciberaula.com/articulo/linux_apache_intro/ . 1 de mayo 2012
- Frank morales .tipos de investigación. Disponible en: http://manuelgross.bligoo.com/conozca-3-tipos-de-investigacion-descriptiva-exploratoria-y-explicativa . 1 de mayo 2012
- Debían.org. instalación de sistema operativo .Disponible en: http://cdimage.debian.org/debian-cd/6.0.5/amd64/iso-cd/debian-6.0.5-amd64-netinst.iso . 30 de abril 2012