RESUMEN

Según los estudios realizados por investigadores en la red mundial, en los últimos años se ha observado un incremento de ataques en las Organizaciones y empresas. Algunos ataques han podido ser detectados pero otros, sin embargo, han podido eludir los mecanismos de seguridad adoptados por las organizaciones, aprovechándose de alguna vulnerabilidad del sistema no conocida por los sistemas de seguridad.

En este contexto, los sistemas honeypots tienen el objetivo de reunir información sobre la actividad del intruso, además aprender cuanto más sea posible de las amenazas y del comportamiento que tienen los atacantes. Los sistemas de honeypots no tienen el propósito de resolver los fallos o errores de seguridad en la red pero son los que se encargan de suministrar la información necesaria sobre los posibles atacantes antes de que comprometan los sistemas reales.

En el presente proyecto se realizó un sistema de honeypots para un estudio de las técnicas utilizadas por los atacantes. Este sistema está conformado por una máquina trampa o equipo víctima, a la cual un intruso la podrá atacar sin necesidad de entrar al sistema de producción, y una máquina de control la cual se encargo de la monitorización y análisis de todos los eventos ocurridos en el equipo víctima.

Por último tras haber detectado el sistema de honeypots un ataque, se realizó un análisis forense el cual consiste en recopilar la información detallada de las acciones realizadas por el atacante, este análisis permite detectar nuevos patrones de ataques y herramientas, antes de que tengan una mayor difusión. De esta forma se podrá advertir a los responsables o administradores de la red de las organizaciones para que tomen las medidas oportunas.

CAPÍTULO I

GENERALIDADES

1.1 Introducción

Tradicionalmente, la naturaleza de la seguridad informática ha sido puramente defensiva, ya que la operación del enemigo informático esta siempre al ataque.

Los muros de fuego, sistemas de detección de intrusos, y el cifrado son mecanismos que se usan defensivamente para proteger los recursos informáticos.

La idea de realizar el presente proyecto de investigación aplicada consiste en defender la infraestructura de información, tan bien como sea posible, detectar posibles fallos en la estructura defensiva y reaccionar a esos fallos de manera proactiva.

El sistema de honeypot aplicado en el presente proyecto está formado por una máquina trampa o equipo víctima, a la cual un intruso podrá atacar, y una máquina de control, la cual se encargará de monitorizar y analizar, de forma transparente, todos los eventos ocurridos en la máquina trampa.

En el proyecto se aplicarán conocimientos de seguridad informática, tácticas, técnicas y procedimientos para irrumpir de manera no autorizada a bóvedas de información electrónica que podrían contener información potencialmente sensible.

1.2 Justificación e Importancia

La necesidad de desarrollar el presente proyecto es identificar, evitar y, en cierta medida, neutralizar los intentos de apropiarse de sistemas y redes de información.

Siendo un proyecto de investigación aplicada, requiere crear toda la documentación que permitirá el buen entendimiento del desarrollo del mismo.

Con las herramientas utilizadas en este proyecto y que actualmente existen se puede realizar un desarrollo completo e integral, a costos medios.

Por los motivos mencionados se hace imprescindible en la actualidad crear una herramienta que permita reducir la atracción de los diferentes atacantes a los sistemas y redes de información.

1.3 Objetivos

1.3.1 Objetivo General

Desarrollar pruebas de un sistema de Honeypots para la detección de intrusos en una red de área local con herramientas basadas en código libre.

1.3.2 Objetivos Específicos

- Analizar el funcionamiento de un sistema Honeypots y puesta en marcha en una red de área local.

- Analizar protocolos y herramientas de software libre para un sistema de Honeypots.

- Diseñar un prototipo para un sistema de Honeypots para una red de área local.

- Realizar pruebas sobre el diseño realizado para un sistema de Honeypots.

1.4 Alcance

El alcance de este proyecto de investigación se desarrollo de un sistema de Honeypots que permitió detectar con facilidad los posibles ataques en una red de área local e ir contribuyendo a la evolución y desarrollo de estándares para la seguridad de las redes.

- Análisis del funcionamiento y las bases técnicas de un sistema de Honeypots.

- Estudio de las funcionalidades que puede poseer un sistema, manteniendo una coherencia con los requerimientos propios de una red estable.

- Análisis de los protocolos que funcionen correctamente con un sistema de Honeypots.

- Comparación de los servicios requeridos para un sistema constante de Honeypots.

- Estudio de herramientas de distribución libre útiles para el desarrollo de un sistema de Honeypots y seleccionar la que presente mayores beneficios.

- Planteamiento con los requerimientos analizados un prototipo para el sistema bajo herramientas de distribución libre para una red de área local.

- Implementación los servicios mas importantes: DNS, WEB, SSH, TELNET, MAIL, FILTRADO DE TRAFICO.

- Realización de pruebas del funcionamiento del sistema de Honeypots, ejecutando las diversas operaciones que permitan al sistema una mejor aplicación, y que a la vez se consolide en un sistema robusto y seguro para las redes de área local.

1.5 Metodología

La Metodología aplicada en el presente proyecto es la metodología de investigación, la cual se caracteriza porque busca la aplicación o utilización de los conocimientos que se adquieren.

A continuación se detalla las fases con las que consta el proyecto de investigación, cada una de ellas con unos objetivos bien definidos.

En la primera fase se describen las tecnologías y herramientas que han servido de precedente para la realización del presente proyecto de tesis.

Se describe el sistema de log de linux: syslog, con el objetivo de conocer el porque de las modificaciones realizadas sobre el código fuente.

En la segunda fase se refiere a la arquitectura del sistema implementada. Se describió la estructura de red, los equipos utilizados y el software y herramientas instaladas en los equipos. En el software, se describió el paquete de instalación de la máquina de control creado para la puesta en marcha de una manera sencilla y transparente del sistema.

Durante la tercera fase se desarrolló un módulo de control, el cual permite la monitorización de las conexiones entrantes y salientes, los ficheros de configuración, los servicios que se van a implementar y la ejecución de los procesos en el sistema, enviando la información remotamente a la máquina de control.

La ultima fase del proyecto consistió en la elaboración del análisis forense a una máquina atacada en la red que se implementó la arquitectura propuesta en la fase dos, y en la que se instaló las herramientas desarrolladas en la fase tres. Se describió además la herramienta utilizada para el análisis forense.

CAPÍTULO II

MARCO TEÓRICO

2.1 Modelo OSI

2.1.1 Introducción al Modelo OSI

En ocasiones el manejo y la transmisión de los datos resulta distorsionada, por lo que la mayoría de usuarios deben asegurarse que sus datos se entreguen y reciban de manera segura y adecuada.

Es aquí donde el Modelo de Referencia de Interconexión de Sistemas Abiertos (Modelo OSI) cobra su importancia y permite que diversos sistemas de cómputo se interconecten e interoperen entre sí, cumpliendo diferentes reglas ya preestablecidas para su total desempeño.

2.1.2 Conceptos Del Modelo OSI

El Modelo OSI, fue creado por la ISO [1] en el que pueden modelarse o referenciarse diversos dispositivos que reglamenta la ITU[2] con el fin de poner

[1] **ISO:** Organización Internacional para la Estandarización
[2] **ITU:** Unión Internacional de Telecomunicaciones

orden entre todos los sistemas y componentes requeridos en la transmisión de datos, así mismo simplificar la relación entre fabricantes.

Es así, que todo dispositivo de cómputo y telecomunicaciones puede ser referenciado al modelo y por consiguiente concebido como parte de un sistema dependiente con características muy precisas en cada nivel.

2.1.3 Estructura del Modelo OSI

El modelo OSI está estructurado de la siguiente manera:

- ***Estructura multinivel*:** Se diseñó este tipo de estructura con el propósito de que cada nivel se dedique a resolver una parte del problema de comunicación, es decir que cada nivel ejecuta funciones específicas.

  El nivel superior utiliza los servicios de los niveles inferiores:

  Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora.

- ***Puntos de acceso****:* Entre los diferentes niveles existen interfaces llamadas "puntos de acceso" a los servicios.

- ***Dependencias de Niveles****:* Cada nivel es dependiente del nivel inferior y también del superior.

- ***Encabezados***: En cada nivel, se incorpora al mensaje un formato de control, el cual permite que un nivel en la computadora receptora esté informada de que su similar en la computadora emisora está enviándole información.

  El mensaje que es enviado está constituido de dos partes:

  Encabezado e Información, es por esto que la incorporación de encabezados es necesaria aunque representa un espacio extenso de información, lo que implica que un mensaje corto pueda ser voluminoso.

  Sin embargo, como la computadora destino retira los encabezados en orden inverso a como fueron incorporados en la computadora origen, finalmente el usuario sólo recibe el mensaje original.

  - **Unidades de información:** En cada nivel, la unidad de información tiene distinto nombre y estructura.

2.1.4 Niveles del Modelo OSI

El modelo OSI es conocido porque ofrece una sencilla explicación de la relación entre los complejos componentes de hardware y los protocolo de red. En el modelo OSI, la capa inferior corresponde al hardware y las capas sucesivas al software que usa la red.

A continuación en la figura 2.1 se indica los niveles de referencia del Modelo OSI.

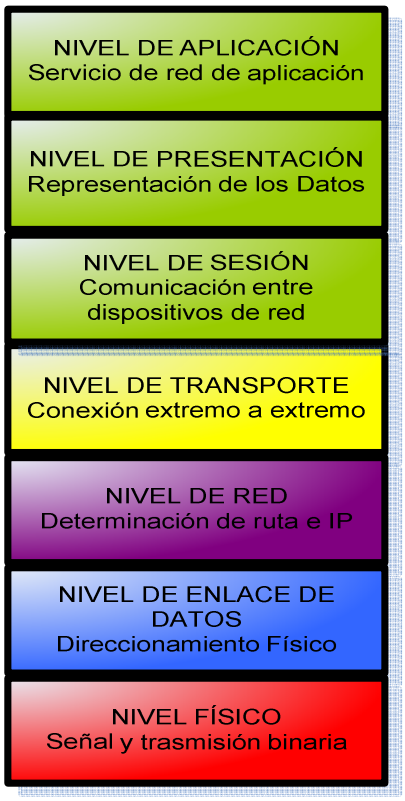


Figura2. 1: Modelo de Referencia OSI

Seguidamente se detallan los niveles o capas del modelo de referencia OSI.

2.1.4.1 Nivel Físico – Capa 1

Es el primer nivel del modelo OSI y en él se definen y reglamentan todas las características físicas-mecánicas y eléctricas que debe cumplir el sistema para poder operar.

Como es el nivel más bajo, se va a encargar de las comunicaciones físicas entre dispositivos y de cuidar su correcta operación.

Se dice que la capa Física transmite el flujo de bits sobre un medio físico y aquella que representa el cableado, las tarjetas y las señales de los dispositivos.

2.1.4.2 Nivel de Enlace de Datos – Capa 2

Conocido también como nivel de Trama, es el encargado de preparar la información codificada en forma binaria en formatos previamente definidos por el protocolo a utilizar.

Tiene su aplicación en el contexto de redes WAN y LAN ya que como se estableció previamente la transmisión de datos no es más que el envío en forma ordenada de bits de información.

Este nivel ensambla los datos en tramas y las transmite a través del medio.

Es el encargado de ofrecer un control de flujo entre tramas, así como un sencillo mecanismo para detectar errores.

2.1.4.3 Nivel de Red – Capa3

Este nivel define el enrutamiento y el envío de paquetes entre redes. De igual manera se encarga de establecer, mantener y terminar las conexiones.

Este nivel proporciona el enrutamiento de mensajes, determinando si un mensaje en particular deberá enviarse al nivel 4 (Nivel de Transporte) o bien al nivel 2 (Enlace de datos).

Este nivel conmuta, enruta y controla la congestión de los paquetes de información en una red.

2.1.4.4 Nivel de Transporte – Capa4

En este nivel se realiza y garantiza la calidad de la comunicación, ya que asegura la integridad de los datos.

Aquí se realizan las retransmisiones cuando la información fue corrompida o porque alguna trama (de la capa 2) detectó errores en el formato y se requiere volver a enviar el paquete o datagrama.

El nivel de transporte notifica a las capas superiores si se está logrando la calidad requerida.

2.1.4.5 Nivel de Sesión – Capa 5

Este nivel es el encargado de proveer servicios de conexión entre las aplicaciones, tales como iniciar, mantener y finalizar una sesión. De igual manera establece, mantiene, sincroniza y administra el diálogo entre aplicaciones remotas.
La capa de Sesión es un espacio en tiempo que se asigna al acceder al sistema por medio de un login en el cual obtenemos acceso a los recursos del mismo servidor. La información que utiliza nodos intermedios que puede seguir una trayectoria no lineal se conoce como "sin conexión".

2.1.4.6 Nivel de Presentación – Capa 6

Se refiere a la forma en que los datos son representados en una computadora. Proporciona conversión de códigos y reformateo de datos de la aplicación del usuario.

Es decir que la capa de Presentación es aquella que provee representación de datos, mantiene la integridad y valor de los datos independientemente de la representación.

2.1.4.7 Nivel de Aplicación – Capa 7

Es el nivel más cercano al usuario y a diferencia de los demás niveles, por ser el más alto o el último, no proporciona un servicio a ningún otro nivel.

Proporciona comunicación entre dos procesos de aplicación, tales como: programas de aplicación, aplicaciones de red, etc.

Así mismo provee de aspectos de comunicaciones para aplicaciones específicas entre usuarios de redes como son: manejo de la red, protocolos de transferencias de archivos (FTP), etc.

La capa de Aplicación se dice que es una sesión específica de aplicación, es decir, son los programas que ve el usuario.

En el desarrollo del proyecto, se considero la implementación de algunos servicios útiles, los mismos que se encuentran dentro de la capa de aplicación correspondiente al modelo OSI.

2.2 Puertos, Protocolos y Servicios.

La finalidad de tener seguridad en una red es que los usurarios de los sistemas informáticos de una organización puedan hacer un mejor uso de los mismos mejorando de este modo el rendimiento global de la organización

Así las organizaciones obtienen una serie de ventajas del uso de las redes en sus entornos de trabajo, como pueden ser: Mayor facilidad de comunicación, mejora de la competitividad, mejora de la dinámica de grupo, reducción del presupuesto para proceso de datos, es así que dentro de la seguridad de la red, existen servicios, protocolos y puertos, que hacen del rendimiento de la red, un acceso más seguro de la información.

Un protocolo es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación, dentro de los protocolos de red tenemos: SSH, SMTP, SSL, FTP, UTP, HTTP, TELNET, cada uno de los cuales tiene su funcionalidad, las cuales se verán más adelante.

De igual manera, en el momento que el ordenador se conecta a Internet, éste pasa a ser un elemento más dentro de la red, es decir, forma parte de toda la red y como tal se tiene que comunicar con el resto. Para poder comunicarse, lo primero que necesita es tener una dirección electrónica y poder identificarse con los demás. Por ejemplo si uno realiza una petición de una página Web, el servidor

tiene que saber a quien se la envía, es por esto que se establece un número de puerto. Así por ejemplo, un servidor Web escucha las peticiones que le hacen por el puerto 80, un servidor FTP lo hace por el puerto 21, etc.

Para que todo esto sea posible, la red debe prestar una serie de servicios a sus usuarios, como son: acceso, ficheros, impresión, correo e información, cada uno con sus características principales, los que prestarán al usuario mayor seguridad dentro de la red.

Dentro de los servicios a usarse están:

2.2.1 Protocolo HTTP

El protocolo de transferencia de hipertexto es el protocolo usado en cada transacción de la Web (WWW[3]). HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. Al finalizar la transacción todos los datos se pierden. Por defecto HTTP escucha en el puerto 80 en el servidor Web.

El protocolo HTTP es el que da vida a Internet, y gracias al cual, los clientes y servidores se pueden comunicar. El funcionamiento básico es que el cliente establece una conexión TCP/IP con el servidor, hace una petición, el servidor le

[3] World Wide Web: Es un sistemas de documentos de hipertexto y/o hipermedios enlazados y accesibles a través de Internet.

responde y se cierra la conexión.

2.2.2 El protocolo SSH

SSH, o "Secure Shell" es tanto una aplicación como un protocolo, que permite conectar dos ordenadores a través de una red, ejecutar comandos de manera remota y mover ficheros entre los mismos. Realmente los datos recibidos sobre este puerto serán reenviados a la máquina remota a su puerto de escucha que por defecto es el número 22.

SSH Proporciona autentificación y comunicaciones sobre canales no seguros y pretende ser un reemplazo tangible para aplicaciones tradicionales no convincentes, como TELNET, RSH y RCP.

De igual forma este protocolo permite solventar problemas de seguridad que pueden derivarse del hecho de que usuarios tengan acceso como administrador a ordenadores de la red, o acceso al cable de comunicaciones, de modo que puedan interceptar contraseñas que se transmiten por la red. Esto no ocurre con SSH, ya que nunca envía texto plano, sino que la información siempre viaja cifrada.

Entre las características de este protocolo están:

- Permite a los usuarios registrarse en sistemas de host remotamente a través del intérprete de comandos.

- Encripta la sesión de registro, no permite que alguien pueda obtener acceso a la información.

2.2.3 Protocolo Telnet

El protocolo Telnet es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente (sistema compuesto de una pantalla y un teclado) con un intérprete de comandos del lado del servidor. En la actualidad lo normal es que las conexiones Telnet se hagan vía Internet, usando el puerto 23.

El protocolo Telnet se aplica en una conexión TCP/IP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet.

Hay tres razones principales por las que Telnet no se recomienda para los sistemas modernos desde el punto de vista de la seguridad:

- Los dominios de uso general del Telnet tienen varias vulnerabilidades descubiertas sobre los años, y varias más que podrían aún existir.

- Telnet, por defecto, no cifra ninguno de los datos enviados sobre la conexión (contraseñas inclusive), así que es fácil interferir y grabar las comunicaciones, y utilizar la contraseña más adelante para propósitos maliciosos.
- Telnet carece de un esquema de autentificación que permita asegurar que la comunicación esté siendo realizada entre los dos anfitriones deseados, y no interceptada entre ellos.

2.2.4 Protocolo SMTP:

SMTP es un es Protocolo Simple de Transmisión de Correo. Este protocolo es el estándar de Internet para el intercambio de correo electrónico, de forma predeterminada SMTP escucha en el puerto 25.

SMTP necesita que el sistema de transmisión ponga a su disposición un canal de comunicación fiable y con entrega ordenada de paquetes, con lo cual, el uso del protocolo TCP en la capa de transporte, es lo adecuado.

Para que dos sistemas intercambien correo mediante el protocolo SMTP, no es necesario que exista una conexión interactiva, ya que este protocolo usa métodos de almacenamiento y reenvío de mensajes.

2.2.5 Protocolo HTTPS

HTTPS es un protocolo seguro de transferencia de hipertexto, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de

hipertexto, es decir, es la versión segura de HTTP. Por defecto el protocolo HTTPS escucha las peticiones en el puerto 443.

El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP.

Cabe mencionar que el uso del protocolo HTTPS no impide que se pueda utilizar HTTP. Razón por la cual el navegador le advierte sobre la carga de elementos no seguros (HTTP), los cuales están relacionados a un entorno seguro (HTTPS).

Los protocolos HTTPS son utilizados por navegadores como: Safari, Internet Explorer, Mozilla Firefox, Opera y Google Chrome, entre otros.

2.2.6 Protocolo SSL

El protocolo SSL es un sistema de seguridad, utilizado actualmente por la mayoría de empresas que comercian a través de Internet. Por defecto SSL escucha en el puerto 443 del servidor de aplicaciones.

Es un sistema de seguridad ideado para acceder a un servidor garantizando la confidencialidad de los datos mediante técnicas de encriptación modernas.

Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes

y, opcionalmente, autenticación de cliente para conexiones TCP/IP.

Dentro de las características de SSL están:

- *Confidencialidad*: Mediante el uso de la Encriptación se garantiza que los datos enviados y recibidos no podrán ser interpretados por ninguna otra persona que no sea ni el emisor ni el receptor.

- *Integridad*: Se garantiza que los datos recibidos son exactamente iguales a los datos enviados, pero no se impide que al receptor la posibilidad de modificar estos datos una vez recibidos

- *Autenticación*: El vendedor se autentifica utilizando un Certificado Digital emitido por una empresa llamada Autoridad Certificadora, éste documento es totalmente infalsificable y garantiza que el Vendedor es quien dice ser.

2.2.7 Protocolo DNS

El Servidor de Nombres de Dominio (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. El puerto que utiliza el DNS para comunicarse con la capa de Aplicación es el número 53.

Aunque como base de datos el DNS es capaz de asociar diferentes tipos de

información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP.

El sistema de nombres de dominios en Internet es un sistema distribuido, jerárquico, replicado y tolerante a fallas. Para la operación práctica del sistema DNS se utilizan tres componentes principales:

- Los Clientes DNS: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS

- Los Servidores DNS: Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada;

- Y las zonas de autoridad, porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

2.3 Firewalls

Los Firewalls son barreras creadas entre redes privadas y redes públicas como por ejemplo, Internet.

Los Firewalls examinan todo el tráfico de entrada y salida, y así permiten el paso solamente al tráfico autorizado, es por esto que se definen entonces ciertas políticas de seguridad las que son implementadas a través de reglas en el firewall donde estas políticas típicamente se diseñan de forma que todo lo que no es expresamente autorizado, es prohibido por defecto.

Un Firewall en sí, protege la red interna de una organización, de los usuarios que residen en redes externas, permite el paso entre las dos redes a sólo los paquetes de información autorizados y puede ser usado internamente, para formar una barrera de seguridad entre diferentes partes de una organización.

Un Firewall de nivel de red permite un control de acceso básico y poco flexible, pues permite aceptar o denegar el acceso basándose sólo en la información que conoce a nivel de red.

2.3.1 Firewall por software

Este tipo de firewall es el más común y utilizado, ya que se trata de un software que instalamos en nuestro ordenador, por lo que sólo va a proteger al ordenador en el que está instalado.

Tal como se explico en la definición, un Firewall tiene la misión de filtrar el tráfico de la red, ya sea de entrada o de salida, para de esta manera evitar intrusiones no deseadas en el ordenador o bien la salida de datos del mismo.

En el mercado hay una gran variedad de programas de este tipo, tanto independientes como formando parte de un paquete junto a un antivirus.

2.3.2 Firewall por hardware

Este tipo de Firewall se trata de un tipo de dispositivo instalado en un periférico parecido a un router. Es una muy buena solución cuando se habla de una red, ya que permite hacer toda la configuración de Firewall en un solo punto al que se conectan los ordenadores.

2.4 Honeypots

Desde los primeros incidentes de seguridad, la principal tarea de los sistemas informáticos ha sido la constante defensa en contra de ataques que pongan en riesgo a los sistemas de las organizaciones.

Esto ha reducido considerablemente la capacidad de aprender de este tipo de sucesos, de manera que en la mayoría de los casos, solo se conocen algunas de las herramientas utilizadas por los atacantes, y pocas veces se conoce como es

que estas herramientas se utilizan en contra de la seguridad de los sistemas de información.

Un Honeypot tiene como objetivo reunir información sobre la actividad del intruso; de esta manera se podrá detectar una vulnerabilidad antes de que sea explotada, además de conocer los riesgos a los cuales los sistemas de producción están expuestos.

Esta es una de las ideas principales en el que se centra Honeypot, aprender cuanto sea posible de las amenazas y del comportamiento de los atacantes, para implantar una arquitectura de seguridad proactiva que le permita no solo defender de tales amenazas, si no también someterlas antes de que sucedan.

2.4.1 Conceptos de Honeypots

Un Honeypot es un recurso de red destinado a ser atacado o comprometido. De esta manera, puede ser explorado, atacado y probablemente comprometido por cualquier atacante.

Los Honeypots no poseen en ningún caso el propósito de resolver o arreglar fallos o errores de seguridad en la red, pero son los encargados de suministrar información valiosa sobre los posibles atacantes en potencia a la red antes de que comprometan sistemas reales.

De igual forma están diseñados como trampas que se utilizan para identificar y evitar los diferentes intentos de apropiarse de sistemas y redes de información.

Existen puntos importantes de los Honeypots que se deben tomar en cuenta:

- Los Honeypots no sirven para eliminar o corregir fallos o errores de seguridad que existan en la red. Si la red es vulnerable, añadir un Honeypot no solventará este fallo.

- Por otro lado, en lugar de evitar a cualquier precio que un atacante fije su interés en la red, le invitamos, incitamos o permitimos a que entre y ataque la red.

Generalmente un honeypot puede ser una computadora o un sitio de red que parecen ser parte de una red pero que en realidad están aislados, protegidos y monitorizados, y que parecen contener información o recursos que serían valiosos para los posibles atacantes.

2.4.2 Importancia de los Honeypots

La seguridad es la reducción de riesgo. No se puede eliminar el riesgo, pero la seguridad ayuda a minimizarlo.

Se puede dividir los mecanismos de seguridad en tres categorías:

1. ***Prevención***: Son aquellos mecanismos que aumentan la seguridad del sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones de la seguridad.

2. ***Detección***: Son aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación.

3. ***Reacción o recuperación:*** Son aquellos mecanismos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su estado de funcionamiento correcto.

Los sistemas honeypots no ofrecen ningún servicio, simplemente son dispositivos que han sido diseñados para ser comprometidos, y atacados, es decir, que el tráfico dirigido a estos sistemas será escaso, por lo que casi con total seguridad, el tráfico dirigido hacia el sistema será producido por un posible ataque al sistema, algún intento de intrusión o algún escaneo con el objetivo de obtener información sobre el sistema.

Si el tráfico es generado por el honeypot seguramente indicará que la máquina ha sido atacada. Por lo tanto todo el tráfico que se genere en el honeypot, tanto como origen o como destino, será sospechoso.

2.4.3 Funciones de los Honeypots

Dentro de las funciones que se centra un Honeypots se puede observar los siguientes puntos:

- Desviar la atención del atacante de la red real del sistema, de tal forma que no se comprometan los recursos principales de la información dentro de la red.

- Capturar nuevos virus o gusanos para un estudio posterior.

- Conformar perfiles de atacantes y sus técnicas de ataque utilizadas con frecuencia, de manera similar a la usada por una corporación policíaca para construir el archivo de un criminal basado en su modus operandi.

- Conocer nuevas vulnerabilidades y riesgos de los distintos sistemas operativos, entornos y programas las cuales aún no se encuentren debidamente documentadas

2.4.4 Ubicación de los Honeypots

La ubicación de los Honeypots es muy importante ya que de esta manera se puede maximizar la seguridad, es decir, debido a su carácter pasivo una ubicación de difícil acceso eliminará gran parte de su atractivo para posibles atacantes.

Por otro lado, si su ubicación es demasiado obvia cualquier potencial atacante la descubrirá y evitará todo contacto con ella.

Se establece tres puntos básicos para acoger los Honeypots según las necesidades:

Antes Del firewall. Esta localización permite evitar el aumento de los riesgos inherentes a las instalaciones de los Honeypots. Como se encuentra fuera de la zona protegida por el firewall, puede ser atacado sin ningún tipo de peligro o problema para el resto de la red.

En la figura 2.2 que se muestra a continuación se puede observar que la instalación del Honeypot se encuentra desprotegido del firewall por lo que está más propenso a ser atacado con más facilidad.

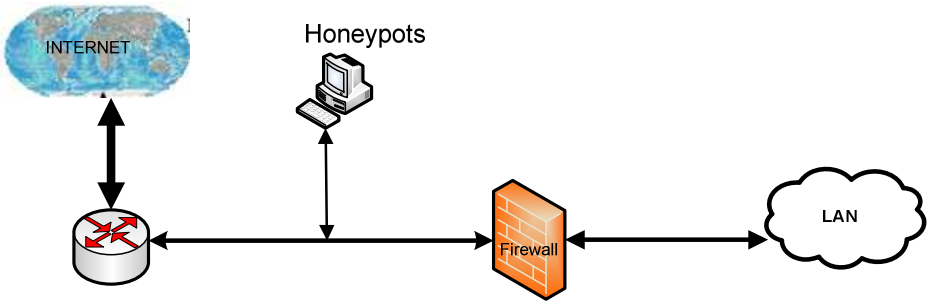


Figura2. 2: Honeypot antes del Firewall

Esta localización permite tener un acceso directo a los atacantes, ya que el firewall se encarga de filtrar una parte del tráfico peligroso o no deseado, logrando

trazas reales de su comportamiento y estadísticas muy confiables de la cantidad y calidad de ataques que se puede recibir en la red.

Esta ubicación evita la detección de atacantes internos. El principal problema que presenta esta localización es que tiene limitaciones en el control del atacante es decir, si le permite un cierto número de conexiones, en casos extremos; es posible que todas y cada conexión sea un ataque exitoso y las medidas de contingencia habrían fracasado.

***Detrás del firewall*.** En esta ubicación, el Honeypot queda afectado por las reglas de filtrado del firewall.

Por una parte se tiene que modificar las reglas para así permitir algún tipo de acceso al Honeypot por posibles atacantes externos, y por el otra parte, al introducir un elemento extremadamente peligroso dentro de la red se puede permitir a un atacante que tenga acceso al Honeypot un paseo triunfal por toda la red.

Esta ubicación tras el firewall permite la detección de atacantes internos así como firewalls mal configurados, máquinas infectadas por gusanos o virus e incluso atacantes externos.

En la siguiente figura 2.3 se puede observar que la configuración del Honeypot se encuentra protegida por el firewall, de manera que se podrá detectar los intrusos antes de que pueda atacar al sistema de honeypot

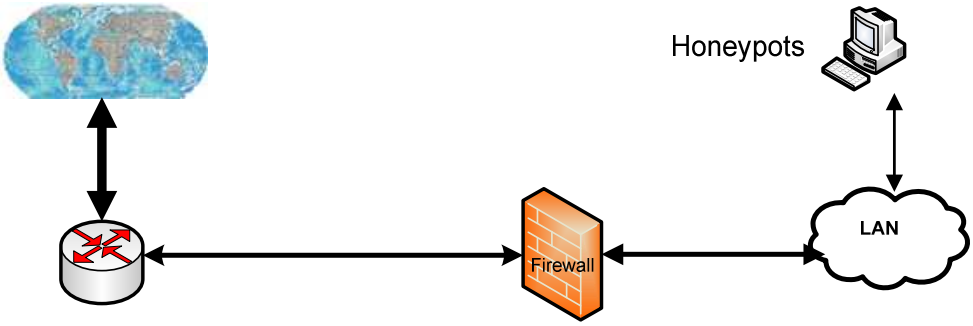


Figura2. 3: Honeypot detrás del Firewall

***En la zona desmilitarizada*:** La ubicación en la zona desmilitarizada permite por un lado agrupar en el mismo segmento a los servidores de producción con el Honeypot y por el otro controlar el peligro que incrementa su uso, ya que tiene un firewall que lo aísla de resto de la red local.

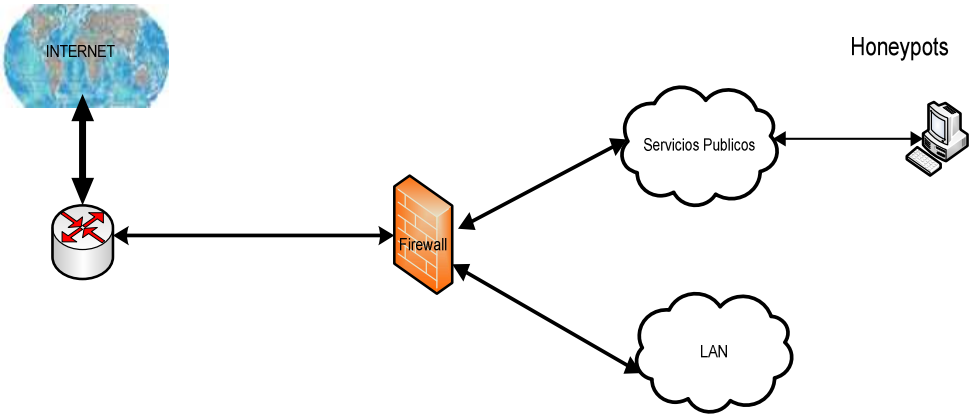


Figura2. 4: Honeypot en Zona Desmilitarizada

En la figura 2.4 se puede observar que el sistema de Honeypot se encuentra detrás del firewall lo que le protege de intrusos pero al mismo tiempo está separado de la red LAN lo que produce que la configuración de Honeypot esté más propenso a ser atacado y desconfigurado.

Esta localización permite la posibilidad de detectar ataques externos e internos con una simple reconfiguración del sistema de firewall puesto que se encuentra en la zona de acceso público.

La detección de atacantes internos se ve algo débil, ya que al no compartir el mismo segmento de red que la LAN, un atacante local no podrá acceder al Honeypot.

Sin embargo, desde la red local sí es posible acceder al Honeypot, ya que si un atacante interno que se encuentre intentando atacar los servidores públicos u otros sistemas externos (ejemplo: un gusano) muy probablemente acabe siendo detectado.

2.4.5 Clasificación de los Honeypots

Los Honeypots se pueden clasificar de acuerdo a su Ambiente de Implementación el cual hace fácil entender su operación y utilización al momento de planear la implementación de uno de ellos dentro de la red de datos.

2.4.5.1 Honeypot de Producción

Este tipo de honeypots ayudan a minimizar los riesgos de una organización, los mismos que añaden nuevas características a las medidas de seguridad. Así mismo se encargan de detectar ataques y disuadir a los atacantes.

Hay que tener en cuenta que los sistemas honeypots de producción no pueden prevenir intrusiones de los atacantes.

Los únicos procedimientos y mecanismos de prevención a utilizar para evitar posibles ataques son la desactivación de los servicios innecesarios, actualizando aquellos que sean inseguros o utilizando mecanismos fuertes de autenticación.

A pesar de que los honeypots no puedan prevenir los ataques del sistema, si puede alejar a posibles atacantes de él, ya que mientras están atacando al sistema honeypot, no están atacando al sistema real.

Una vez que se haya descubierto al atacante, se comunica al resto del sistema para que se tomen las medidas correctas como: denegar cualquier acceso con un origen determinado, limitar las capacidades de un servicio, paralizar varios servicios momentáneamente.

2.4.5.2 Honeypot de Investigación

Este tipo de honeypots están diseñados para obtener información de los atacantes, no añaden ninguna característica de seguridad a una organización, solamente son utilizados en la investigación de nuevos mecanismos de intrusión en los sistemas.

Su principal objetivo es el de recoger información sobre los diferentes atacantes así como de sus comportamientos y técnicas asociadas.

Ofrecen servicios reales e incluso pueden llegar a permitir que el atacante informático tome total control del equipo.

2.4.6 Ventajas y Desventajas de los Honeypots

2.4.6.1 Ventajas de los Honeypots

***Obtención de datos importantes*.** Los sistemas honeypots recogen una cantidad pequeña de datos, pero de gran importancia. Es por esto que hace que el número de falsas alarmas sea muy pequeño y que todos los datos almacenados sean importantes. En otros mecanismos de seguridad se almacenarán mucha cantidad de información pero el porcentaje de información importante será muy bajo.

Los recursos no son saturados. Muchas herramientas o mecanismos de seguridad pueden ser saturados por la gran cantidad de información que deben analizar. Es por esto que algunos sistemas de detección de intrusos basados en red pueden ser colapsados en periodos de mucho tráfico en la red que están analizando, con la pérdida de paquetes y con ello posibles ataques no detectados.

También los mecanismos de almacenamiento en los ficheros log pueden verse saturados por una gran cantidad de eventos producidos en el sistema, perdiendo alguno de estos eventos de gran importancia.

Sin embargo, los sistemas honeypots no tendrán este problema ya que solamente capturarán la información referente a ellos, y como se ha dicho antes que la cantidad de información recogida por estos sistemas es poca, entonces no llegarán a saturarse.

2.4.6.2 Desventajas de los Honeypots

Necesitan ser atacados. Todo sistema Honeypot necesita ser atacado para poder cumplir la funcionalidad para el cual ha sido instalado. Si no son atacados no son de gran utilidad.

Riesgo. Los sistemas honeypots pueden introducir riesgo en el entorno donde se implante. Dependiendo del tipo de sistema que utilice el riesgo será mayor o menor.

Debido a las desventajas de los sistemas honeypots, éstos no pueden reemplazar ningún mecanismo de seguridad de la organización donde se implante.

Los sistemas honeypots solamente podrán añadir ciertas características a las medidas de seguridad existentes en la organización.

2.4.7 Fases de la Seguridad de la Información

FASE DE PREVENCIÓN

La prevención en cualquier sistema de seguridad se centraliza en evadir que los atacantes logren su objetivo.

Un *Honeypot* suministra un valor mínimo en la prevención de los diferentes ataques. Sin embargo, existen dos posibles usos de los *Honeypots* en la prevención:

1. *Decepción*: Su principal objetivo es hacer perder tiempo al enemigo, estableciendo distintos sistemas que fingen contener información de producción.

Se trata de confundirlos, atrasar su proceso y decepcionarlos eventualmente, logrando así detener sus ataques.

2. *Disuasión*: Su principal característica es atemorizar al atacante. Si el enemigo se enterara de que existen sistemas Honeypots mezclados con sistemas en producción, podrían analizar perfectamente antes de atacar y correr el riesgo de ser detectados.

FASE DE DETECCIÓN

Su principal objetivo es detectar y advertir acerca de cualquier actividad no autorizada.

En las redes el mayor valor se centra en la detección, ya que de esta manera se permite capturar actividad altamente valiosa y reducir falsos positivos los cuales por error del software o antivirus reportan que el área del sistema está infectada, cuando en realidad el objeto esta limpio de virus y falsos negativos el cual mediante un error del software falla en detectar un archivo o área del sistema que en realidad esta infectada.

Así mismo, al no contar con tráfico de producción, toda interacción es fruto de accesos no autorizados, logrando así detectar ataques no conocidos, independientemente de la táctica, técnica o herramienta que se utilice.

FASE DE RESPUESTA

Después que se haya detectado un ataque de cualquier enemigo, los sistemas de seguridad deben estar preparados para responder inmediatamente.

La correcta respuesta a un incidente dentro de la seguridad de la información, se complica cuando el enemigo utiliza una nueva herramienta o técnica, las diferentes actividades del atacante se confunden con el tráfico de producción o los sistemas de producción no se pueden aislar para su análisis, pues deben continuar suministrando el servicio.

A pesar que los Honeypots, no cuentan con tráfico de producción, no se ven afectados por los problemas ya mencionados, ya que poseen una capacidad de detectar ataques desconocidos, por lo que lo convierte en una herramienta muy útil para detectar rápidamente ante nuevos enemigos.

Toda empresa u organización debe contar con una política de seguridad que implique los procesos a ejecutar en las tres categorías y solo así se podrá explotar al máximo el potencial de los sistemas Honeypots.

2.4.7.1 Escenarios de Aplicación de los Honeypots

La aplicación de los Honeypots ante los distintos ataques se puede llevar a cabo en dos escenarios, el uno que se encuentra orientado a fortalecer la seguridad de

ambientes en producción y el otro que se encuentra encaminado a la investigación.

Escenario de Producción

Los Honeypots en este escenario, se implantan en ambientes en producción, como por ejemplo en la infraestructura de red de una entidad financiera o gubernamental.

Sin embargo, esto no quiere decir que las redes de trampa (Honeypots) procesen tráfico de producción.
Generalmente se instalan en el mismo ambiente de los sistemas en producción, esperando así atraer a los atacantes para que las analicen, ataquen o comprometan.

Existen algunas de las formas en las que un honeypot ayuda a reforzar la seguridad dentro de la empresa u organización.

1. Cuando el honeypot detecta un ataque, en primer lugar se procede a examinar las herramientas y tácticas que se estén utilizando y después se refuerza los sistemas de seguridad para que el ataque no afecte a los sistemas de producción.

2. Cuando el atacante complica a un honeypot, este se analiza en detalle para así buscar patrones en sistemas de producción y determinar si alguno de los sistemas también fue comprometido.

Es así que los Honeypots representan una herramienta muy flexible y orientada a recopilar únicamente tráfico producido por accesos no autorizados y que al ser administrada por una política de seguridad de la entidad, permite prevenir, detectar y responder a los distintos ataques que se susciten.

Escenario de Investigación

Aquí los Honeypots se implantan para cumplir dos objetivos: investigar las tácticas, herramientas y motivos de la comunidad *black-hat*[4]; y compartir las lecciones aprendidas.

Dentro de la seguridad de la información existe un inconveniente que es el poco conocimiento acerca de los atacantes y sus tácticas. Los Honeypots aplicados a la investigación se enfocan en detectar los diferentes ataques, en generar y compartir el conocimiento para que las diferentes organizaciones fortalezcan su infraestructura.

[4]**Black Hat:** Métodos y técnicas que no son legales para posicionarse en los buscadores pero que sirven para adquirir una mejor posición en los resultados de los buscadores

2.5 Sistemas Honeypots

Entre los principales sistemas de honeypots tenemos los siguientes:

2.5.1 Backofficer Friendly

BACKOFFICER FRIENDLY (BOF) es un honeypot muy simple pero altamente útil. Es un programa que funciona en la mayoría de sistemas operativos basados en ventanas. Todo lo que puede hacer es emular algunos servicios básicos, tales como HTTP, FTP, TELNET, CORREO.

Siempre que se producen intentos de conexión en uno de los puertos BACKOFFICER FRIENDLY que están escuchando, entonces se registrará el intento. Este tipo de sistema también tiene la posibilidad de falsificar respuestas, por lo que el atacante pensará que está conectado a un determinado servicio.

De esta manera se registran ataques de tipo Web o una variedad de otras actividades. La característica principal de este tipo de sistemas es la detección.

Este tipo de honeypot puede supervisar solamente un número limitado de puertos, que a menudo representan los servicios más comúnmente explorados y atacados.

2.5.2 Specter

Este tipo de sistema es similar al BOF ya que emula servicios, pero éste puede emular una mayor cantidad de servicios y tiene más funcionalidades.

Además, puede emular no sólo servicios, sino también emular una variedad de sistemas operativos., es fácil de poner en ejecución y de poco riesgo. Specter puede instalarse en sistemas que tengan Microsoft Windows como sistema operativo.

Como Specter puede emular diferentes sistemas operativos, entonces se reduce el riesgo pues no hay un sistema operativo real con el cual el atacante interactúa. Por ejemplo, Specter puede emular un servidor Web o un servidor Telnet del sistema operativo que le indiquemos.

Cuando el atacante intenta conectarse a alguno de estos servidores e intenta obtener alguna página Web u otra información, entonces estas actividades son capturadas y registradas por Specter, no obstante el atacante poco más podrá hacer ya que los servicios no son reales y su funcionalidad está emulada.

La característica más importante de Specter es la detección, ya que puede determinar rápidamente y fácilmente quién está husmeando en el sistema. Como honeypot, reduce falsos positivos y falsos negativos.

Otra característica importante de este sistema es que permite la obtención de información, o capacidad automatizada de recopilar más información sobre el atacante.

2.5.3 Homemade

Este tipo de honeypot captura una actividad específica, tal como gusanos o actividades de escaneos. Éstos pueden utilizarse como honeypots de producción o de investigación, dependiendo de su propósito.

Los Honeypots Homemade pueden modificarse para hacer (y emular) mucho más, requiriendo un nivel más alto del complejidad, e incurriendo en un nivel más alto de riesgo.

Algunos ejemplos adicionales de honeypots Homemade son:

- Port listener. Usado para capturar el gusano de W32/Leaves.
- Emulador de Windows Inetd para Windows NT y Windows 2000.
- LaBrea Tarpit. Es una aproximación a los honeypots, que no solamente nos permite capturar la actividad de un gusano, sino también inhabilitar dicho ataque.

2.5.4 Honeyd

Este sistema está diseñado para funcionar en sistemas Unix, puede emular unos 400 sistemas operativos diferentes y miles de diversos ordenadores, todos en el mismo tiempo.

Honeyd introduce nuevas características. Primero, emula no sólo sistemas operativos en el nivel de aplicación, como Specter, sino que también emula sistemas operativos en el nivel de la pila del protocolo IP. Esto significa que cuando alguien está escaneando puertos o servicios en el sistema honeypot, el servicio y la pila IP se comporta como el servicio del sistema operativo que estamos emulando.
En segundo lugar, Honeyd puede emular miles de diferentes tipos de ordenadores en el mismo tiempo. Mientras que la mayoría de los honeypots pueden emular solamente una computadora en un momento determinado, Honeyd puede asumir la identificación de miles de direcciones IP al mismo tiempo.

Y en tercer lugar, se trata de un sistema honeypot *open source*, con lo que ello supone. Honeyd se utiliza sobre todo para detectar ataques. Trabaja supervisando las direcciones IP que el sistema no tiene asignadas.

Honeyd detecta y registra las conexiones hechas a cualquier puerto. La capacidad de asumir un sistema que no existe, y la capacidad de detectar cualquier actividad

en cualquier puerto, es por esto que se da a Honeyd un valor increíble como herramienta para detectar actividades no autorizadas.

2.5.5 Mantrap

Este sistema en vez de emular servicios, Mantrap crea hasta cuatro subsistemas, a menudo llamados cárceles. Estas cárceles son sistemas operativos lógicamente discretos separados de un sistema operativo principal.

Los administradores de seguridad pueden modificar estas cárceles durante el funcionamiento normal, para incluir la instalación de la base de datos Oracle o el servidor Web Apache, por ejemplo.

Esto hace al sistema honeypot más flexible. El atacante tiene un sistema operativo completo con el cual interactuar, y una variedad de servicios y herramientas a atacar. Toda esta actividad después se captura y se registra.

Este honeypot se puede utilizar como un honeypot de producción o como un honeypot de investigación para aprender más sobre amenazas. Actualmente, Mantrap solamente está soportado en el sistema operativo Solaris.

2.5.6 Honeynets

Este tipo de honeypots puede obtener información sobre las amenazas que existen en la comunidad de Internet hoy en día.

Un Honeynet es una red de sistemas de producción. En este tipo de honeypot nada será emulado, a diferencia del resto de honeypots que se mencionaron.

Prácticamente no se realiza ninguna modificación en el sistema honeypot a analizar. Esto da a los atacantes una gama completa de sistemas y aplicaciones donde poder atacar.

Sin embargo, con esta capacidad el riesgo asumido es mucho mayor, y por lo tanto deberán tomarse unas medidas para evitar que una vez comprometido el honeynet, éste no pueda atacar a otros sistemas.

	CARACTERÍSTICAS
Backofficer Friendly **Specter**	• Funciona en la mayoría de sistemas operativos basados en ventanas. • Emula algunos servicios básicos, tales como HTTP, FTP, TELNET, CORREO. • Registra ataques de tipo Web o una variedad de otras actividades. • Funciona en sistemas que tengan Microsoft Windows como sistema operativo. • Emula mayor cantidad de servicios y tiene más funcionalidades. • Emula una variedad de sistemas operativos. • Determina rápidamente y fácilmente quién está intentado acceder al sistema • Tiene capacidad automatizada de recopilar más información sobre el atacante.
Homemade	• Captura una actividad específica, tal como gusanos o actividades de escaneo. • Pueden modificarse para realizar y emula mucho más actividades.
Honeyd	• Funciona en sistemas Unix • Emula sistemas operativos tanto en el nivel de aplicación,

	como en el nivel de la pila del protocolo IP. • Emula miles de diferentes tipos de ordenadores en el mismo tiempo. • Detecta y registra las conexiones hechas a cualquier puerto.
Mantrap	• Funciona solamente en el sistema operativo Solaris. • Crea hasta cuatro subsistemas, es decir, sistemas operativos lógicamente discretos separados de un sistema operativo principal.
Honeynets	• Obtiene información sobre las amenazas que existen en la comunidad de Internet hoy en día. • Nada será emulado. • No se realiza ninguna modificación en el sistema honeypot a analizar.

Cuadro 2. 1: Características de los HoneyPots

Se escogió Honeynet ya que mediante este sistema honeypot se puede obtener información de las amenazas que existen hoy dentro de la red, a pesar de que este sistema tiene mayor riesgo de ser atacado, recobra mucha más información sobre posibles atacantes.

Una de las principales características de este sistema es que son sistemas y aplicaciones reales, los mismos que puede encontrar en Internet. Nada es emulado ni se hace nada para que los sistemas sean menos seguros. Los riegos y vulnerabilidades encontradas en una Honeynet son las mismas que existen hoy en muchas organizaciones. Uno simplemente puede tomar un sistema de un entorno comercial y situarlo dentro de una Honeynet.

2.6 Honeynet

Es un honeypot más complejo de alta interacción con el intruso y que permite coleccionar mayor cantidad de información en un ataque, con la finalidad de aprender sobre las herramientas, tácticas y motivos que alientan a este tipo de usuarios.

Honeynet captura y controla mediante un firewall todo el tráfico destinado a los equipos dentro de la misma, para que de esta forma se haga un análisis posterior el cual permita tener mayor conocimiento de las intrusiones.

Honeynet es diferente de los honeypots tradicionales, es lo que se cataloga como un honeypot para la investigación. Esto no lo hace una mejor solución que los honeypots tradicionales, simplemente tiene un propósito diferente.

Esto significa que cuando un intruso es detectado lo que hace honeynet es recopilar información de las posibles amenazas.

Las dos principales diferencias de diseño respecto a los honeypots tradicionales son:

- No es un sólo sistema sino una red de varios sistemas y aplicaciones las cuales son investigadas y atacadas.

- Todos los sistemas situados dentro de una Honeynet son sistemas comerciales estándar. Estos son sistemas y aplicaciones reales, los mismos que puede encontrar en Internet. Nada es emulado ni se hace nada para que los sistemas sean menos seguros.

  Los riegos y vulnerabilidades encontradas en una Honeynet son las mismas que existen hoy en muchas organizaciones. Uno simplemente puede tomar un sistema de un entorno comercial y situarlo dentro de una Honeynet.

El objetivo de toda Honeynet es el obtener información tanto de las amenazas que atentan contra los sistemas de información, así como del comportamiento de los intrusos y sus motivos

2.6.1 Requerimientos de Honeynet

Dentro de los requerimientos de Honeynet se debe contemplar tres elementos críticos para su correcta implementación:

- Captura de datos
- Control de datos
- Recolección de datos

2.6.1.1 Captura de Datos

Todo el tráfico de entrada y salida, así como la actividad en cada equipo dentro de la Honeynet debe de ser registrado para su posterior análisis. Uno de los puntos más importantes en la captura de datos es la descentralización de los mecanismos de captura.

Esto quiere decir, que deben de existir una infraestructura de captura por capas, de manera que si un sistema de captura de datos llegase a fallar, no esté todo perdido.

Para que un intruso llegue a los Honeypots, tiene que pasar por el firewall (comúnmente implantado como un firewall invisible) en el cual se tiene el primer registro de la actividad hacia la Honeynet.

Después de esto, debido a que el firewall permite todo el tráfico de entrada hacia la Honeynet, el router funciona como una segunda capa, en la que podremos obtener algunos datos sobre la actividad hacia los Honeypots, y además existe un

detector de intrusos que le ayudará a obtener información identificada como un escaneo o algún ataque.

2.6.1.2 Control de Datos

El control de datos dentro de Honeynet permite limitar el tráfico que salga desde la misma, debido a que si un equipo es comprometido, teniendo que evitar que sea utilizado para comprometer a otros sistemas que se encuentran fuera de la Honeynet.

Sin embargo esto podría delatar el propósito del equipo al cual el intruso ha entrado, de manera que cuando se de cuenta que la actividad hacia la red está limitada, el equipo no será de su interés y podría borrar toda la evidencia que ha generado, y se perdería la oportunidad de aprender más sobre el intruso.

Una manera de evitar esto, es permitir cierta cantidad de tráfico desde la Honeynet hacia el exterior, además de limitar los servicios a los cuales se puede conectar desde la Honeynet.

Se puede configurar el firewall de manera que permita la salida de cierta cantidad de tráfico de servicios predefinidos, de manera que se pueda obtener más información sobre el comportamiento del intruso. Sin embargo mientras más tráfico se permita desde la Honeynet hacia el exterior mayor será el riesgo que se tenga de causar problemas a otros equipos.

2.6.1.3 Recolección de Datos

La recolección de datos consististe en la reunión de información de varias Honeynets de manera centralizada.

No es muy común encontrar este punto en el diseño de una Honeynet debido a que es para proyectos que incluyen varias Honeynets en diferentes partes de una ciudad, país o del mundo.

Se debe contar con un medio seguro de almacenamiento para recolectar la información de Honeynets distribuidas.
Cada Honeynet deberá enviar la información a un medio centralizado identificándose mediante un ID.

Dentro de los datos podría ser enviados se encuentran los registros de tráfico en modo binario, así como las bitácoras del tráfico de entrada y salida generadas por el firewall.

2.6.2 Arquitectura de Honeynet

En la Arquitectura de las Honeynet existen dos principales generaciones

Primera Generación (Gen I)

El propósito de esta generación de Honeynets, es capturar la máxima cantidad de información de la actividad del intruso, y hacerlo sentir en una red real. Esta arquitectura se subdivide en tres subredes (la Honeynet, la red de producción e Internet) que se encuentran separadas perfectamente por un firewall.

Las medidas de control y captura de datos son sencillas y en algunos casos detectables por el intruso.

En la figura 2.5 que se muestra a continuación de puede observar que el control de todas las redes se realiza mediante un firewall, ya que cualquier paquete de entrada o salida debe pasar obligatoriamente por él, es por esto que el router también se utiliza como medio de control y filtrado, pero únicamente como soporte al firewall.

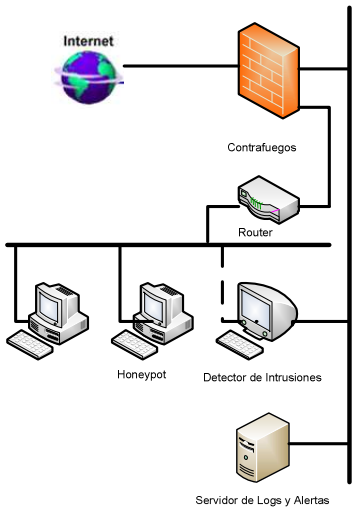


Figura2. 5: Honeynet de la Primera Generación

Segunda Generación (Gen II)

Honeynets de segunda generación se caracterizan por combinar todos los requisitos de la primera generación en un solo dispositivo. De esta forma tanto el control de flujo de datos como la captura y la recolección de datos quedan agrupadas en una misma entidad o en un mismo sistema de la Honeynet.

La finalidad de esta generación es facilitar la implantación de una solución Honeynet, así como hacer más difícil su detección.

Mediante esta arquitectura se obtiene un control total de todas las conexiones que se pueda realizar, independientemente de si su número es mayor, menor o igual al límite existente en las Honeynet de GEN I.

Como se puede observar en la figura 2.6 que el control de todas las redes se realiza mediante un firewall, pero al contrario de la 1era Generación éste se encuentra en capa 2 , el mismo, que trabaja en modo de puente y controla todo el tráfico de entrada y salida de la Honeynet haciendo su detección mas difícil .

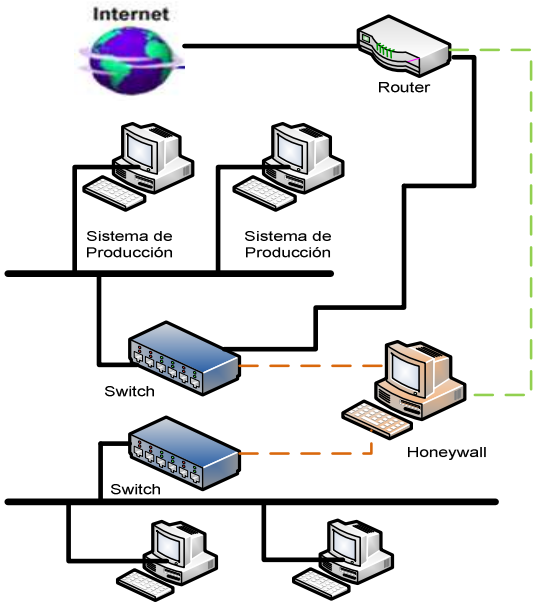


Figura2. 6: Honeynet de la Segunda Generación

De igual manera se puede modificar la actividad del atacante en lugar bloquear simplemente cualquier tipo de acceso no permitido. Así de esta forma, el ataque como tal sale de la Honeynet pero no es efectivo debido a las modificaciones que se pueden realizar en tiempo real sobre el paquete de datos.

2.6.3 Clasificación de Honeynet

Dentro de la clasificación de una Honeynet se puede analizar tres categorías importantes que se encuentran bien diferenciadas, dentro del sistema de detección de intrusos.

2.6.3.1 Honeynet para Investigación

Los Honeynets para investigación consisten en analizar las técnicas utilizadas por los hackers, para comprometer un sistema.

Por lo tanto, uno de los requisitos principales exige que el grado de protección de la *Honeynet* sea máximo, es decir, tan elevado como sea posible, teniendo en cuenta el conocimiento actual de los administradores de la red en materia de seguridad.

Se deben instalar mecanismos de *logging independientes* de la propia *Honeynet* que arrojen pistas acerca de cómo se ha llevado a cabo un ataque exitoso.

También se pueden utilizar para investigar cuáles son las técnicas de ataque más habituales o cuáles son los pasos seguidos por un atacante para recopilar información acerca de los sistemas de la red objetivo.

Estos datos permiten mejorar las políticas de seguridad de los sistemas que están realmente en producción.

2.6.3.2 Honeynet Vulnerables

El principal objetivo de este planteamiento es introducir en Honeynet una vulnerabilidad real y fácilmente identificable por el atacante, con objeto de desviar su atención de las máquinas en producción.

Existen dos requisitos adicionales que deben contemplarse en este tipo de Honeynet.

- El primero de ellos coincide con las honeynet de investigación, es decir que los mecanismos de logging que registren la actividad del atacante deben ser completamente independientes de la máquina que actúa como Honeynet; si este requisito no se cumple, el atacante puede hacer uso de los privilegios que ha obtenido en la Honeynet para anular dichos mecanismos.

- El segundo requisito exige que el entorno de la Honeynet esté protegido, para que el ataque no se propague a otras zonas de la red. Un procedimiento sencillo para cumplir este requisito consiste en colocar delante de la honeynet un firewall que sólo permita el tráfico entre la honeynet y el exterior.

2.6.3.3 Honeynet Aparentemente Vulnerable

En esta categoría se utiliza software de virtualización que permite simular una vulnerabilidad fácilmente identificable.

Es casi similar a la categoría anterior, salvo por el hecho de que en este caso el atacante no consigue realmente su propósito. En su lugar, se le presenta un entorno virtual que simula el comportamiento de una máquina comprometida.

La ventaja de esta categoría, es que el atacante no dispone de privilegios para anular los mecanismos de *logging* ni de los recursos suficientes para propagar el ataque hacia otras zonas de la red.

2.7 Sistemas de Detección de Intrusos (IDS)

La detección de una intrusión consta de dos procesos, el proceso de monitorización de los eventos ocurridos en un sistema informático o una red, y el análisis de los eventos en busca de posibles intrusiones.

Entendemos como intrusión a cualquier intento de comprometer la confidencialidad, integridad y disponibilidad de un sistema o red, así como también los intentos por evitar los mecanismos de seguridad existentes.

Las intrusiones pueden producirse por atacantes que acceden a los sistemas desde Internet, por usuarios autorizados del sistema que intentan obtener privilegios adicionales para los cuales no están autorizados o también por usuarios autorizados que hacen un mal usos de los privilegios asignados.

Así pues, definiremos un sistema de detección de intrusos (Intrusion Detection System, IDS) como una herramienta de seguridad que automatiza los procesos de monitorización y de análisis de los eventos ocurridos en un sistema informático o una red de ordenadores, en busca de posibles intentos de intrusión en el sistema.

Debido al incremento de los ataques producidos en los últimos años, muchas organizaciones han decidido añadir sistemas de detección de intrusos en la infraestructura de seguridad de su organización, permitiéndoles de esta manera proteger sus sistemas de las amenazas existentes en la red.

A continuación veremos algunas razones por las cuales muchas organizaciones usan este tipo de sistemas:

- Disuadir individuos que intentan atacar el sistema.
- Detectar ataques y otras violaciones de seguridad que no son prevenidas por otras medidas de protección, como por ejemplo los firewalls.
- Detectar preámbulos de ataques.
- Estos sistemas pueden actuar como control de calidad de las medidas de seguridad tomadas en el sistema y poder documentar las amenazas existentes en la organización.

2.8 Seguridad Informática

En la actualidad, las empresas u organizaciones son cada vez más dependientes de sus redes informáticas y este es un verdadero problema, por mínimo que sea, ya que puede llegar a comprometer la continuidad de las operaciones.

La ausencia de medidas de seguridad en las redes es una realidad que está cada vez más en crecimiento. Está aumenta el número de atacantes los cuales se

encuentran mejor organizados, de manera que van obteniendo mayor cantidad de habilidades que les permiten tener mayores beneficios.

Tampoco se debe dejar de lado los ataques de seguridad provenientes del interior mismo de la empresa u organización. La propia complejidad de la red es una dificultad para la detección y corrección de la cantidad y múltiples problemas de seguridad que van apareciendo.

En seguridad informática la mayoría del mundo desconoce la magnitud del problema con el que se está enfrentando, y generalmente no se invierte ni en capital humano, y muchos menos en capital económico necesarios para prevenir el daño o la pérdida de la información.

2.8.1 Conceptos de la Seguridad Informática

En la actualidad, la seguridad informática ha adquirido gran incremento, dados los cambios de condiciones y las nuevas plataformas de computación disponibles.

La posibilidad de interconectarse a través de redes, ha abierto nuevas y grandes perspectivas que permitirán explorar más allá de las fronteras de la empresa u organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados y en las redes de las organizaciones.

Las políticas de seguridad informática (PSI) surgen como una herramienta dentro de la organización para concienciar a cada uno de los miembros de la misma sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

Es así que la seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Así mismo la Seguridad Informática es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

2.8.2 Estándares de la Seguridad Informática

Los estándares de seguridad informática son instrumentos que han permitido a las distintas herramientas informáticas poder interactuar y la base de la interoperabilidad informática. Son los que han permitido definir cómo interactuaran los miles o millones de componentes informáticos que existen. Los estándares tienen especificaciones públicas y accesibles a un precio simbólico.

Sin embargo, estándares existen de muchos tipos y según de cuál de ellos se esté hablando, se estarán garantizando unas funcionalidades y capacidades de

interoperabilidad técnica informáticas distintas. A continuación se detallan algunos de los estándares de seguridad informática más relevantes:

Para la administración de seguridad de la información:

- La Internet Engineering Task Force (IETF) elaboró el RFC2196 Site Security Handbook, que ofrece una guía práctica para quienes intentan asegurar servicios e información.

- El estándar británico BS 7799 es un estándar aceptado ampliamente que ha sido utilizado como base para elaborar otros estándares de seguridad de la información, incluyendo el ISO 17799[5] y el ISO 27001[6]. Fue desarrollado por el British Standards Institute.

- La Organización para la cooperación y el desarrollo económicos en ingles (OECD) creo las Guidelines for the Security of Information Systems. Directrices de la OCDE para la seguridad de sistemas y redes de información.

Estándares para evaluación de seguridad en sistemas:

- La International Organization for Standardization (ISO) ha elaborado el estándar IS 15408. Este estándar, The Common Criteria for Information

[5] ISO 17799**:** Es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar e implantar o mantener la seguridad de una organización.
[6] ISO 27001: Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Technology Security Evaluation v2.1 (ISO IS 1540 es una mezcla mejorada de ITSEC, el Canadian Criteria, y el US Federal Criteria.

- La Serie Arco Iris - Rainbow Series- (Orange Book) (EE.UU.) Una importante serie de documentos es la Rainbow Series, que delinea varios estándares de seguridad desarrollados en los Estados Unidos.

- El Reino Unido elaboró el Information Technology Security Evaluation Criteria (ITSEC) a comienzos de los años 90, y es otro estándar históricamente importante. Fue elaborado, en algunos aspectos, basándose en el Orange Book.

2.8.3 Objetivos de la Seguridad Informática

Generalmente, los sistemas de información obtienen todos los datos de una empresa u organización, y de igual manera en los recursos de software que permiten a una organización recopilar y hacer circular esta información. Los sistemas de información son fundamentales para las organizaciones y deben ser protegidos.

La seguridad informática consiste principalmente en garantizar que los recursos de software de una organización se utilicen especialmente para los propósitos para los que fueron creados y dentro del marco previsto.

La seguridad informática establece cinco objetivos principales; como se muestra a continuación.

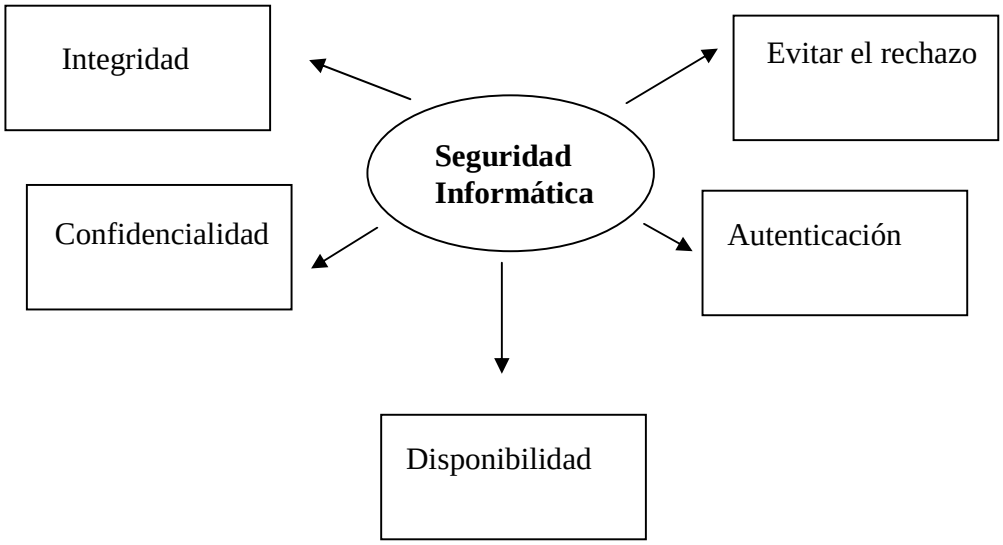


Figura2. 7: Objetivos de la Seguridad Informática

1. **Integridad**. La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

2. **Confidencialidad**. La confidencialidad se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: la intercepción o recepción

electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.

3. **Disponibilidad**. La disponibilidad de la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

4. **Evitar el rechazo**. Constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.

5. **Autenticación**. La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite (por ejemplo gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.

El principal objetivo de la seguridad informática es proteger la información de los sistemas de una manera correcta.

La administración requiere que la información contenida en los sistemas sea integra y sea capaz de tener la certeza para la toma de decisiones

2.8.4 Modelo de Seguridad de Defensa en Profundidad

El concepto de defensa en niveles enseña principalmente que la seguridad es un aspecto transversal, que abarca desde la información misma (los datos) hasta las dependencias físicas donde se encuentra la información, pasando por un conjunto de capas sucesivas y relacionadas. Pero quizá lo más destacable del modelo de defensa en profundidad es que todas estas capas están rodeadas por el aspecto humano: una solución de seguridad que no tenga considerado el aprendizaje del tema por parte de los usuarios está condenado al fracaso. A continuación se detallan las capas del modelo de defensa en profundidad.

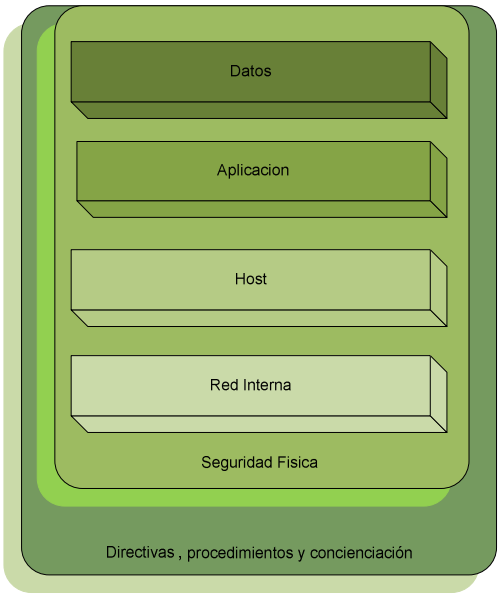


Figura2. 8: Modelo de Seguridad Informática

Datos. El riesgo en esta capa se debe a las vulnerabilidades que un atacante podría aprovechar para obtener acceso a los datos de configuración y

organización, o cualquier dato que sea exclusivo de un dispositivo que utiliza la empresa.

Aplicación. El riesgo en esta capa se debe a las vulnerabilidades que un atacante podría aprovechar para obtener acceso a las aplicaciones en ejecución.

Host. El riesgo proviene de los atacantes que se aprovechan de las vulnerabilidades en los servicios que ofrecen el host o el dispositivo.

Red interna. Los riesgos para las redes internas de las organizaciones están relacionados con los datos confidenciales que se transmiten a través ellas.

***Red perimetral*.** Los riesgos de la capa de red perimetral (también denominada zona desmilitarizada, DMZ o subred protegida) tienen su origen en el posible acceso por parte de un atacante a las redes de área extensa (WAN) y los niveles de red que conectan. Los principales problemas se centran en los puertos TCP (protocolo de control de transmisión) y UDP (protocolo de datagrama de usuario) disponibles que utiliza la red.

Seguridad física. Los riesgos se encuentran en el acceso físico de un atacante a un activo físico.

***Directivas, procedimientos y concienciación*.** Esta capa es la más descuidada y desatendida de todas siendo la más importante siendo el inicio del modelo.

Directivas y procedimientos que la organización necesita establecer a fin de cumplir y admitir los requisitos de cada nivel, la concienciación en la organización de todas las partes interesadas.

2.8.5 Elementos de la Defensa en Profundidad

La defensa en profundidad se establece mediante la combinación adecuada de los elementos siguientes:

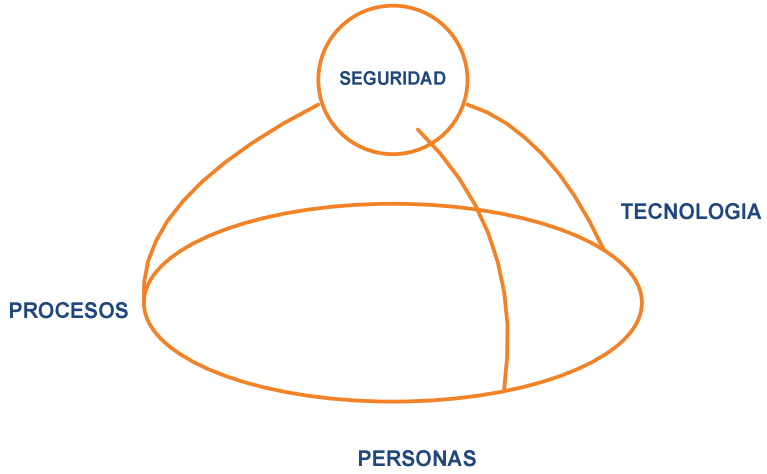


Figura2. 9: Elementos de la defensa en profundidad de seguridad

PERSONAS

Debe implicarse al personal de la empresa empezando por la concienciación de los directivos en la necesidad de gestionar la seguridad.

PROCESOS

Sostener la seguridad de la organización requiere una serie de acciones diarias como: planificar, hacer, verificar y actuar.

TECNOLOGIA

Sin un sistema global de gestión de la seguridad resulta ineficaz y produce una falsa sensación de seguridad, defraudando las expectativas generadas.

2.8.6 Protección de los Sistemas Informáticos

En cualquier sistema informático existen tres elementos básicos a proteger: el hardware, el software y los datos.

Hardware. Conjunto de todos los sistemas físicos del sistema informático. (CPU, cableado, equipos de comunicación.)

Software. Todos los elementos lógicos que hacen funcional al hardware. (SO, aplicaciones, utilidades.)

Datos. Conjunto de información lógica que maneja el software y el hardware. (BD, archivos.)

De los elementos mencionados el más importantes son los datos ya que es el resultado del trabajo realizado.

En caso de que existieran daños en el hardware o en el software estos pueden adquirirse nuevamente desde su medio original, pero la información es difícil de recuperar.

Dentro de la seguridad informática existen una gran cantidad de ataques que se los puede clasificar así:

Ataques Pasivos. Él atacante no altera en ninguna instancia la comunicación, únicamente la escucha y la monitoriza, para así obtener la información que está siendo trasmitida.

Las principales características de este ataque son la intercepción de datos y el análisis de tráfico.

Ataques Activos. Estos ataques son los que involucran algún tipo de modificación del flujo de datos que se trasmiten o la creación de un falso flujo de datos. Los ataques activos pueden tener dos objetivos diferentes: pretender ser alguien que en realidad no lo es para obtener información o colapsar los servicios que se prestan en la red.

2.8.7 Principios de la Seguridad Informática

Para lograr sus objetivos, la seguridad informática se fundamenta en 5 principios que debe cumplir todo sistema informático; los cuales se detallan a continuación.

Figura2. 10: Principios de la seguridad informática

Integridad de la Información

Es uno de los objetivos que hace que su contenido permanezca inalterado a menos que sea modificado por el personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias.

Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informático y/o modificación por personas que se infiltran en el sistema.

Disponibilidad u Operatividad de la información

Capacidad de la información de estar siempre disponible para ser procesada por las personas autorizadas.

Esto significa que el sistema informático, se mantiene funcionando eficientemente y que puede recuperarse rápidamente en caso de fallo, lo contrario significa denegación del servicio de hecho muchos ataques de virus existentes consiste no en el borrado de la información sino en el bloqueo de esta.

Privacidad o Confidencialidad de la Información

Es la necesidad de que la misma solo sea conocida y modificada por personas autorizadas. En caso de que no exista confidencialidad, la información puede provocar grandes daños a su propietario o al igual volverse obsoleta.

Control de la información

Es el que permite asegurar que sólo los usuarios o personal autorizado pueden decidir cuándo y cómo permitir el acceso a la misma.

Autenticidad

El cual permite definir si la información requerida es válida y utilizable en tiempo, forma y distribución. Este objetivo permite asegurar el origen de la información, validando el emisor de la misma, para así evitar suplantación de identidades.

2.9 Herramientas

2.9.1 Linux

Linux es un sistema operativo, compatible Unix. Dos características muy peculiares lo diferencian del resto de sistemas que se puede encontrar en el mercado, la primera, es que es libre, esto significa que no se tiene que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente.

El sistema lo forman el núcleo del sistema (kernel[7]) más un gran número de programas que hacen posible su utilización.

Muchos de estos programas y bibliotecas han sido posibles gracias al proyecto GNU[8], por esto mismo, muchos llaman a Linux, GNU/Linux, para resaltar que el sistema lo forman tanto el núcleo como gran parte del software producido por el proyecto GNU.

Linux se distribuye bajo la GNU General Public License por lo tanto, el código fuente tiene que estar siempre accesible y cualquier modificación ó trabajo derivado tiene que tener esta licencia.

[7] **Kernel ó núcleo** de linux se puede definir como el corazón de este sistema operativo. Es el encargado de que el software y el hardware de tu ordenador puedan trabajar juntos.
[8] **Proyecto GNU**: Proyecto iniciado por Richard Stallman con el objetivo de crear un sistema operativo completamente libre

El sistema ha sido diseñado y programado por multitud de programadores alrededor del mundo. El núcleo del sistema sigue en continuo desarrollo bajo la coordinación de Linus Torvalds, la persona de la que partió la idea de este proyecto, a principios de la década de los noventa.

Hoy en día, grandes compañías, como IBM, SUN, HP, Novell y RedHat, entre otras muchas, aportan a Linux grandes ayudas tanto económicas como de código. Día a día, más y más programas y aplicaciones están disponibles para este sistema, y la calidad de los mismos aumenta de versión a versión.

La gran mayoría de los mismos vienen acompañados del código fuente y se distribuyen generalmente bajo los términos de licencia de la *GNU General Public License*. Más y más casas de software comercial distribuyen sus productos para Linux y la presencia del mismo en empresas aumenta constantemente por la excelente relación calidad-precio que se consigue con Linux.

2.9.1.1 Características Principales

Multitarea: La palabra multitarea describe la habilidad de ejecutar varios programas al mismo tiempo. LINUX utiliza la llamada *multitarea preventiva,* la cual asegura que todos los programas que se están utilizando en un momento dado serán ejecutados, siendo el sistema operativo el encargado de ceder tiempo de microprocesador a cada programa.

***Multiusuario**:* Muchos usuarios usando la misma máquina al mismo tiempo.

***Multiplataforma**:* Las plataformas en las que en un principio se puede utilizar Linux son 386-, 486-. Pentium, Pentium Pro, Pentium II, también existen versiones para su utilización en otras plataformas, como AMD64, Alpha, ARM, MIPS, PowerPC y SPARC.

Multiprocesador: Soporte para sistemas con más de un procesador está disponible para Intel, AMD y SPARC.

Carga de ejecutables por demanda: Linux sólo lee del disco aquellas partes de un programa que están siendo usadas actualmente.

Política de copia en escritura para la compartición de páginas entre ejecutables: Esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse. Cuando alguno intenta escribir en esa memoria, la página (4Kb de memoria) se copia a otro lugar. Esta política de copia en escritura tiene dos beneficios: aumenta la velocidad y reduce el uso de memoria.

Memoria virtual usando paginación **(sin intercambio de procesos completos) a disco:** A una partición en el sistema de archivos, con la posibilidad de añadir más áreas de intercambio sobre la marcha.

La memoria se gestiona como un *recurso unificado* para los programas de usuario

y para el caché de disco, de tal forma que toda la memoria libre puede ser usada para caché y ésta puede a su vez ser reducida cuando se ejecuten grandes programas

2.9.2 Herramientas Open Source

Herramientas Open Source se les conoce como a las herramientas distribuidas y desarrolladas libremente. Este término Open Source fue utilizado por primera vez en 1998 por algunos usuarios de la comunidad del software libre, tratando de usarlo como reemplazo al ambiguo nombre original en inglés del software libre.

Generalmente se piensa que las herramientas Open Source es el "software por el que no hay que pagar" (software gratuito) y, por otro, se adapta al significado que se pretendió originalmente (software que posee ciertas libertades).

Desde el punto de vista tecnológico el "código abierto" está enmarcado dentro de las facilidades para acceder al código fuente y realizar cualquier modificación que a criterio del usuario experto necesite realizarlas, por lo que debido a las circunstancias en que se accede a este código abierto puede ser interpretado como un término más débil y flexible que el del software libre.

Basado en ello se argumenta que una herramienta de código abierto puede ser software libre –software que brinda libertad a los usuarios sobre un producto adquirido, y puede ser estudiado, modificado, copiado, distribuido y usado según

las conveniencias con las que se lo haya adquirido -, pero también puede ser semilibre –software libre pero viene con autorización de uso, copia, modificación y redistribución (incluso de versiones modificadas) sin fines de lucro- incluso completamente no libre -programa informático en el que los usuarios tienen limitadas las posibilidades de usarlo, modificarlo o redistribuirlo, ya que este no está disponible o el acceso a éste se encuentra restringido-.

Hay que tener en cuenta que las herramientas Open Source, que obtienen los usuarios les dan la libertad de ser modificadas o mejoradas, a diferencia de los del software que tiene el código fuente disponible y este en algunas ocasiones se presenta con fuertes restricciones sobre el uso de dicho código.

Generalmente muchos piensan que cualquier software que tenga el código fuente disponible es Open Source, puesto que lo pueden manipular. Sin embargo, mucho de este software no da a sus usuarios la libertad de distribuir sus modificaciones, restringe el uso comercial, o en general restringe los derechos de los usuarios, y de ahí parten las diferentes tipos de distribuciones del software libre.

NOMBRE DE DISTRIBUCIÓN DE SOFTWARE LIBRE	**CARACTERÍSTICAS**
Licencias GPL (*Licencia Pública General GNU*).	El autor conserva los derechos de autor (copyright), y permite la redistribución y modificación, pero controlando que todas las versiones modificadas del software.
Licencias BSD	El autor mantiene la protección de copyright únicamente para la renuncia de garantía y para solicitar la atribución de la autoría en trabajos derivados, pero permite la libre redistribución y modificación, incluso si dichos trabajos tienen

	propietario.
Licencias MPL y Derivadas	Este tipo de licencias de Software libre son muy parecidas a las BSD, pero son menos permisivas.
Copyleft	Se puede interpretar como copia permitida, es decir la autorización por parte del propietario de la licencia para su copia, modificación y posterior distribución.
Freeware	Es un tipo de licencia en el que se autoriza el uso del software de forma libre y gratuita, aunque esta sesión pueda ser bajo determinadas condiciones y en ocasiones suele incluir una cláusula en la que se especifica la prohibición de venta de dicho software, como por ejemplo que el software incluya algún tipo de publicidad o limitación referente al tipo de usuario al que va destinada. Un ejemplo de esto sería que se autoriza su uso a particulares, pero no a empresas o a organismos oficiales.
Shareware	Se autoriza el uso de un programa para que el usuario lo evalúe y posteriormente lo compre. Este software tiene una limitación en el tiempo de utilización o bien una limitación en el funcionamiento de sus funciones y opciones, pero suele tratarse de software operativo.
Demo	Se trata de la sesión de un programa para su evaluación, pero con unas fuertes limitaciones en su desempeño. Un claro ejemplo de esto es un programa que nos permite ver qué se puede hacer con el.
Postcardware	Es un tipo de licencia muy similar al freeware, sólo que suele pedirse el envío de una postal como confirmación de su utilización, aunque la utilización del programa no suele estar supeditada al envío de esta.
Donationware	Se le pide al usuario el envío de un donativo para sufragar el desarrollo del programa, si bien no se supedita ni el uso de este ni sus opciones al envío de dicho donativo
Abandonware	Se trata de software, normalmente con bastante antigüedad, sobre el que sus creadores han liberado el copyright o los derechos de autor. El software afectado por este tipo de licencia suele estar descatalogado y no disponible en tiendas ni otros canales de distribución y venta. Este tipo de licencia se aplica sobre todo a juegos, y si bien

	tuvo bastante éxito a finales de los 90 y principios de 2000, cada vez tiene menos incidencia.

Cuadro 2. 2: Distribuciones de Software Libre

La idea que late detrás del Open Source es bien sencilla y practica: cuando los programadores en Internet pueden leer, modificar y redistribuir el código fuente de un programa, éste evoluciona, se desarrolla y mejora.

Los usuarios lo adaptan a sus necesidades, corrigen sus errores a una velocidad impresionante, mayor a la aplicada en el desarrollo de software convencional o cerrado, dando como resultado la producción de un mejor software.

2.9.2.1 SEBEK

Sebek es una herramienta que permite capturar datos y así recrear con exactitud los acontecimientos en un Honeypot sobre los atacantes y sus técnicas.

La información que se recopila mediante esta herramienta ayuda a determinar cuando un intruso invade en una determinada red de comunicación y la forma en la que lo hizo.

SEBEK permite controlar el rendimiento de lo que el intruso realizó, y de igual forma lo que el usuario ve como salida de información cuando las sesiones no están encriptadas. En el caso de que el período de sesiones este encriptado, el nuevo flujo de los rendimientos de los contenidos codificados del período de

sesiones para poder usarse debe estar descifrado.

El proceso de recopilación de los ataques implica la captura de los datos después de desciframiento la idea es permitir que estos mecanismos estándar de desciframiento permitan proporcionar acceso sin ningún tipo de protección de datos.

Si un archivo es copiado en el honeypot, la herramienta Sebek permite ver y grabar el archivo, convirtiéndose en una copia idéntica.

Esta herramienta, es una de las alternativas de manejo de sesiones de TCP, y también proporciona la capacidad para supervisar el funcionamiento interno de la honeypot. SEBEK puede rastrear las acciones locales de los programas maliciosos, incluso si acceder a la red y rastrear todas las acciones.

Arquitectura de Sebek

Sebek tiene dos componentes: un cliente y el servidor. El cliente captura datos fuera de un honeypot y las exportaciones a la red, donde es reunido por el servidor, como se puedo observar en la *Figura 2.11*.

Dichos servidor agrupa los datos de uno de las dos posibles fuentes: la primera es un paquete de la captura en vivo de la red, la segunda es un archivo de captura de

paquetes almacenados en un archivo con formato de tcpdump[9]. Las comunicaciones utilizadas por Sebek están basadas en UDP y, como tales, son de conexión y poco fiables.

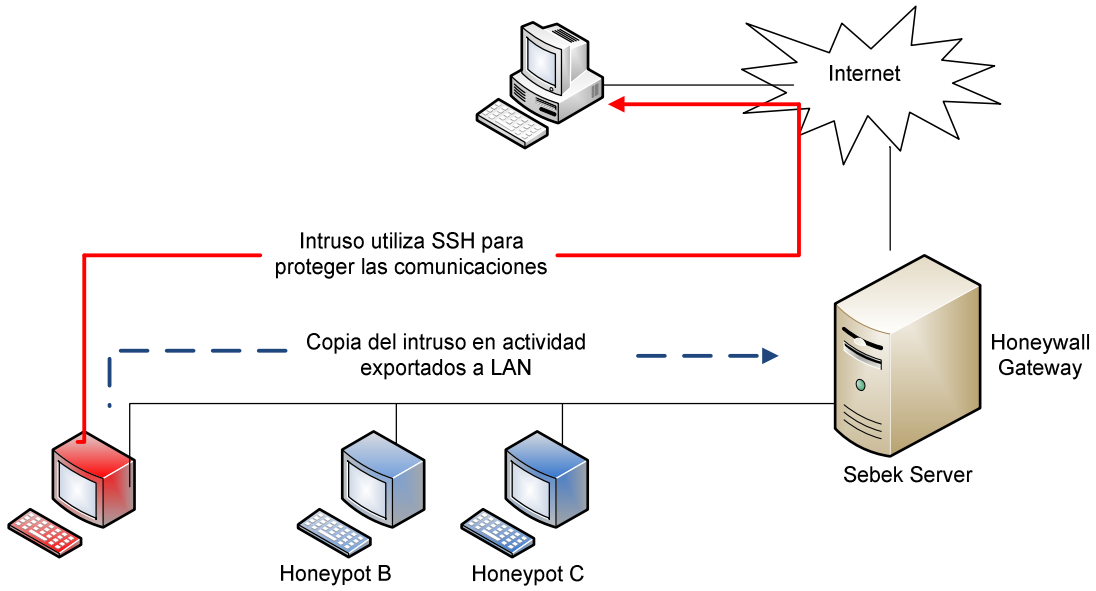


Figura2. 11: Arquitectura de Herramienta SEBEK

Como se puede observar en la figura 2.11 el cliente reside en su totalidad en el kernel. El cliente puede registrar todos los datos de acceso de los usuarios a través de la lectura llamada al sistema. Esta información es luego exportada al servidor a través de la red, de manera que es difícil de detectar desde el honeypot el funcionamiento del Sebek.

2.9.2.2 SNORT

La herramienta Snort es un sniffer de paquetes y así mismo un detector de intrusos basado en red.

[9] Tcpdump: Es un herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red.

Esta herramienta permite capacidades de almacenamiento de la información recopilada dentro de sus bitácoras – historial de archivos de consola que permiten guardar en los logs la información para su posterior análisis dentro de un período de tiempo establecido, además este análisis también se lo puede hacer offline - tanto en archivos de texto como en bases de datos abiertas, como lo es MySQL**.** Implementa un motor de detección de ataques que permite registrar, alertar y responder ante cualquier anomalía previamente definida.

Es pequeño y flexible pero de a poco ha ido adquiriendo funcionalidades las cuales solo se encontraban en los IDS comerciales.

Un verdadero IDS analiza los paquetes, marca las transmisiones que sean potencialmente maliciosas y la almacena en un registro formateado, así, Snort utiliza la librería estándar libcap y tcpdump como registro de paquetes en el fondo.

Esta herramienta Snort está disponible bajo licencia GPL, la cual tiene como propósito declarar que el software cubierto por esta licencia es software libre, gratuito y funciona bajo plataformas Windows y UNIX/Linux.

SNORT es una herramienta subsistema flexible de firmas de ataques ya que posee una base de datos de ataques que se está actualizando constantemente y a la cual se puede añadir o actualizar a través de la Internet.

2.9.2.3 IPTABLES

Es una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log, mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red.

Iptables es una forma de indicarle al kernel algunas acciones que debe hacer con cada paquete, esto se hace en base a las características de un paquete en particular. Los paquetes de red tienen muchas características, algunas pueden ser los valores que tienen en sus encabezados (a donde se dirigen, de donde vienen, números de puertos, etc.), otra puede ser el contenido de dicho paquete (la parte de datos), y existen otras características que no tienen que ver con un paquete en particular sino con una sumatoria de ellos. La idea es lograr identificar un paquete y hacer algo con el mismo.

Debido a que iptables requiere privilegios elevados para operar, el único que puede ejecutarlo es el administrador.

CAPÍTULO III

DESARROLLO DEL SISTEMA

3.1 Introducción al Honeywall CDROM

En el año 2003, se creo el primer CD-ROM Honeywall llamado Eeyore el cual fue expuesto al mundo tecnológico. La intención era hacer Honeynets más fácil de desplegar y personalizar. Con simplemente colocar el CD se lo hace arrancar como un CD booteable, y se lo puede configurar en función de su entorno, se debe tener una puerta de enlace para la configuración del Honeywall. Así mismo, apoya varios métodos de configuración, pero había varios puntos débiles también, los cuales no le permitían una mayor interacción con el usuario y por ende no se sacaba el mayor provecho de este.

En el año 2005, se creo el CD-ROM Honeywall Roo fue expuesto con nuevas mejoras radicales, que combina todas las herramientas y los requisitos de un Honeynet de Tecnología de Tercera Generación. Esta herramienta contiene los principales genios de datos de control y el registro de datos con las funcionalidades agregadas GUI de administración remota, y la integración de análisis de datos.

Con el apoyo de la herramienta Sebek, la cual es un sistema operativo base robusto y su actualización es automática.

Como primer paso se va a construir una Honeynet en una máquina puesta como servidor, compuesto por un P4 2.7 GHz de procesador y 1 GB de RAM.

Para esto se recomienda tener un sistema con al menos P4 1.4 GHz procesador con 1 GB de RAM, por lo que la Honeywall, y el Honeypots se puedan ejecutar correctamente.

Para la creación del Honeypots se utilizó el sistema operativo Fedora 8. Una vez que el sistema operativo está instalado, se procede a la instalación en el Anexo A, el cual permite implementar, personalizar y gestionar el Honeynet con facilidad.

El Honeywall actúa como un puente en capa 2 de gateway que lo captura y posee todo el de la Honeynet. Por ultimo se instalará el atacante en una máquina virtual para poner a prueba la configuración de la Honeynet.

3.2 Arquitectura de Red del Honeywall

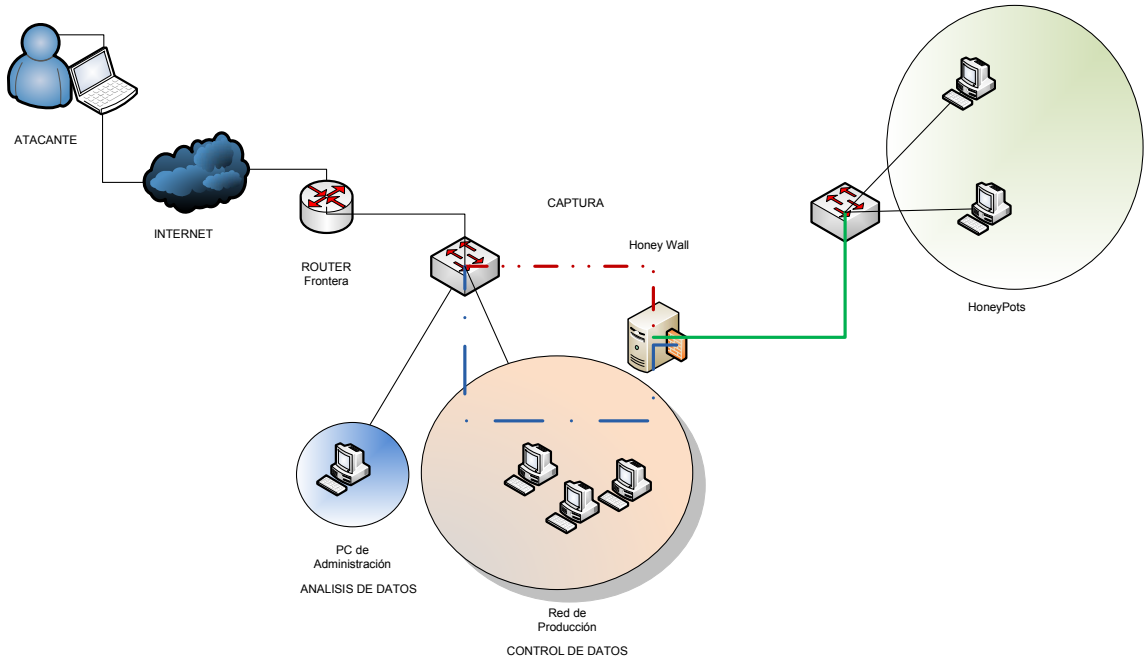


Figura 3. 1: Arquitectura de Red del Honeywall

La arquitectura de red del Honeywall posibilita las opciones de controlar, capturar y analizar todos los datos que son observados. Al momento que un intruso intenta ingresar a la red de producción, esté incrementa las cadenas de datos en la cabecera final que es la que se validará para el ingreso en la red de producción, estas verificaciones necesarias de red se dan tanto a nivel físico como lógico, con ello se habla del conjunto interno que conforma el Honeywall: SEBEK, Iptables, Reglas de Firewall y, SNORT.

Con el Honeywall se restringe todo tipo de acceso a la red de producción y a la información confidencial que en ella se maneja; si se da el caso que exista un intruso estos son redireccionados a las Honeypots, que es conocida como una

trampa de seguimiento de los pasos que efectúo el intruso al querer acceder a la red.

3.3 Instalación de la Herramienta

Dentro de la gama de distribuciones Linux existentes para la seguridad de redes, se ha escogido a la herramienta Roo, en su versión 1.4, que es parte del proyecto HoneyNet, la cual tiene el kernel de la distribución basada en Centos 5.0.

Roo contiene dentro de su instalación una serie de paquetes que le permiten funcionar como un firewall, un sistema de detección de Intrusos (IDS) y de un sistema de alertas que es el que permite la funcionalidad en conjunto del sistema de Honeywall.

Los paquetes que incluye esta versión de Roo, entre los más importantes son:

- Snort
- Iptables
- SEBEK
- Walleye

El proceso de instalación paso a paso se describe dentro del Anexo A.

3.4 Creación de Honeypots con herramientas de Software Libre

Configuración del DNS

Para configurar se modifican los siguientes archivos

1. En el named.conf configurar la zona master y la zona de reversa, la master es el dominio y la reversa es la ip que corresponde a ese dominio.

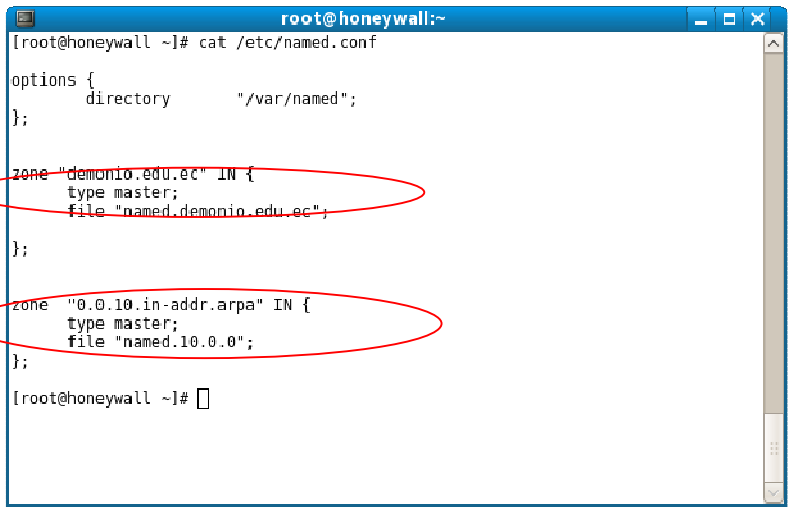


Figura3. 2: Configuración de la zona master y la zona reversa

2. En el named.demonio.edu.ec, se definen los miembros del DNS, por nombres de máquinas.

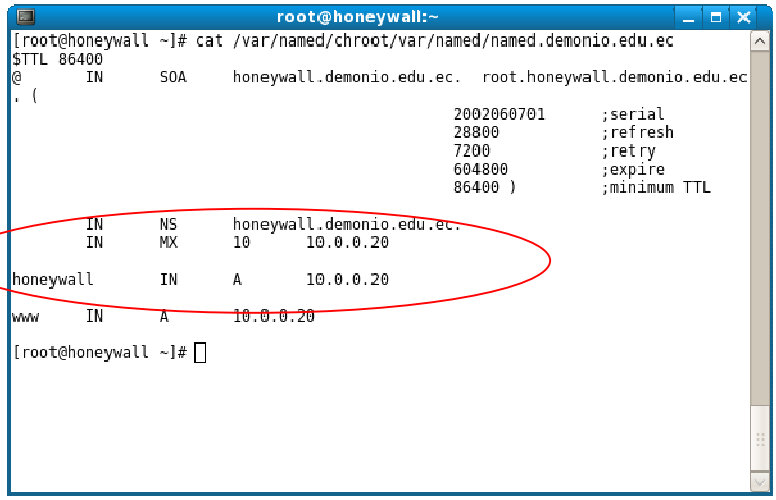


Figura3. 3: Definición de miembros del DNS

3. En named 10.0.0, se define las IPs que corresponden a cada nombre dentro del DNS

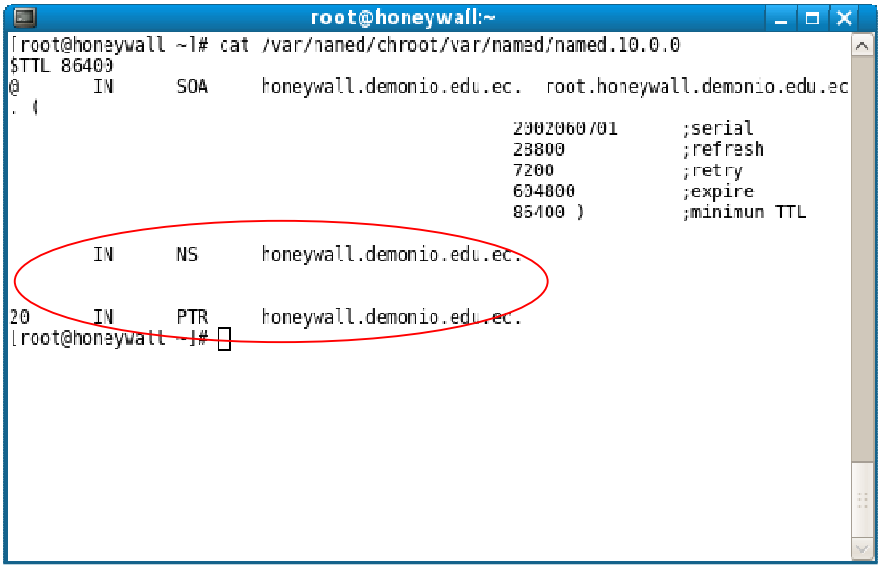


Figura3. 4: Definición de IPs de DNS

4. El archivo localhost.zone define la zona de DNS la máquina.

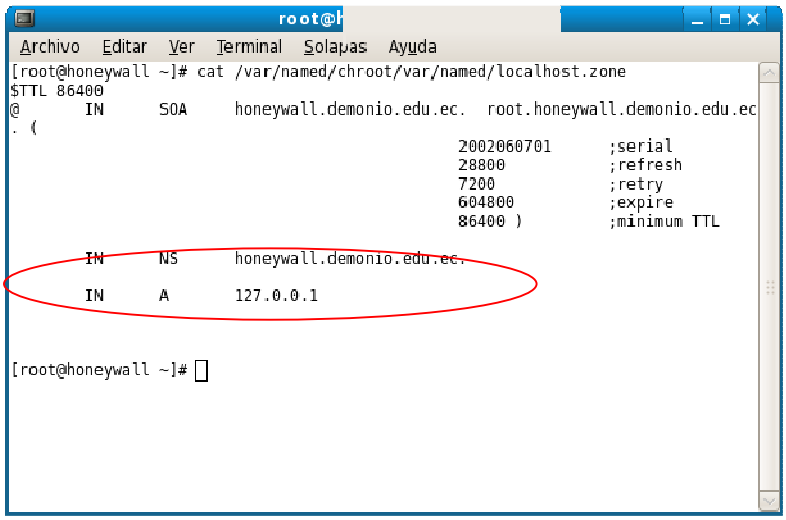


Figura3. 5: Archivo de definición de zona DNS

5. Nombres de la definición de la misma máquina en el archivo named.local

   # service named start

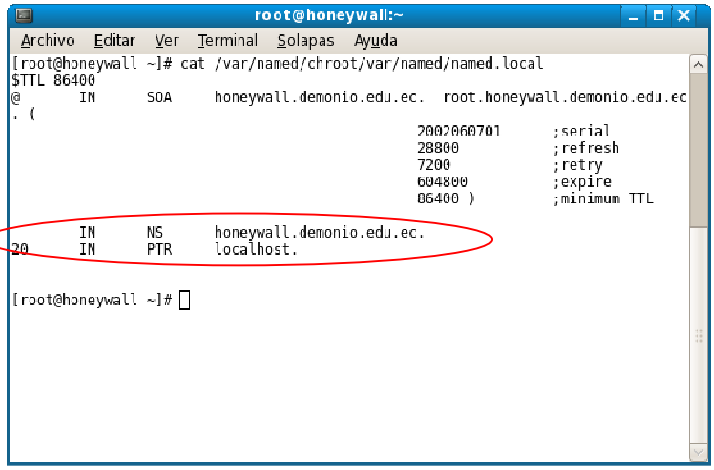


Figura3. 6: Definición del archivo named.local

Configuración de correo sendmail – CORREOS

Configuración dentro del DNS

1. Ir al archivo named.demonio.edu.ec, donde se especifica la maquina donde corre el servicio de correo.

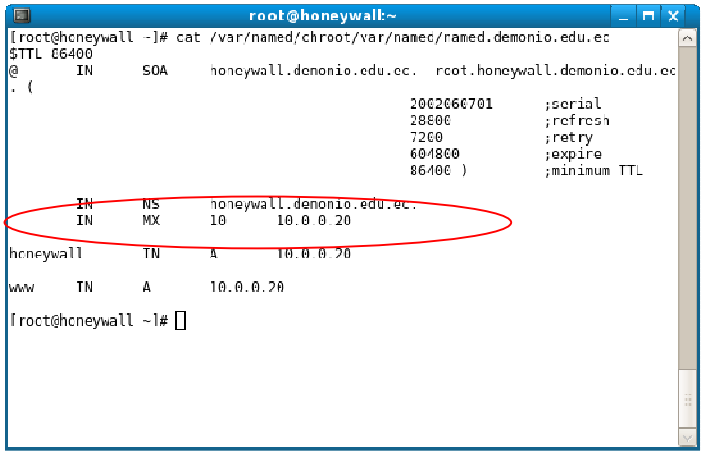


Figura3. 7: Verificación del servicio de correo

service named stop

service named start

2. Configuración sendmail

vim /etc/mail/sendmail.cf

3. Ir a sendmail.cf para definir el dominio de la red y el nombre de la maquina donde corre el servicio de correo.

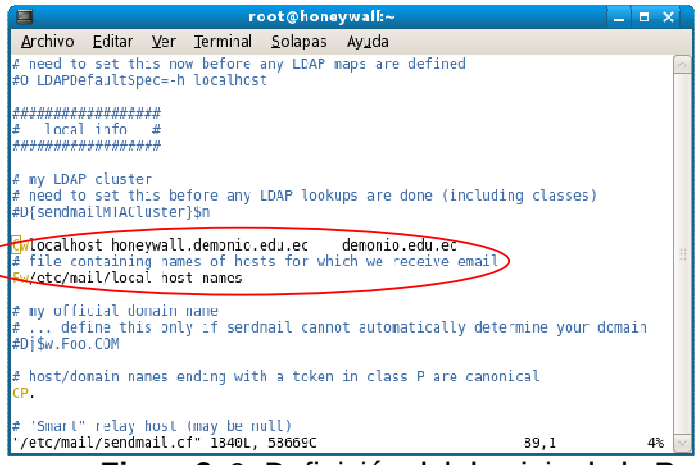


Figura3. 8: Definición del dominio de la Red

service sendmail start

4. Configuración dovecot

vim /etc/dovecot.conf

5. En el dovecot.conf, se define los protocolos con los que trabaja el correo, como son: imap y pop3

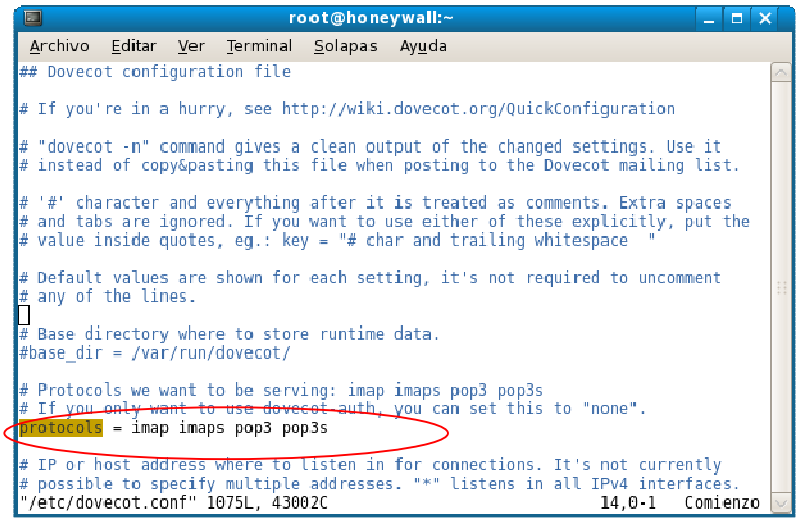


Figura3. 9: Definición de protocolos de correo

service dovecot start

- Iptables

6. Son las seguridades que se da al servidor instalando el paquete iptables, Ir a Sistema, Administración y Cortafuegos y definir aquellos puertos que están abiertos y el resto se los inhabilita.

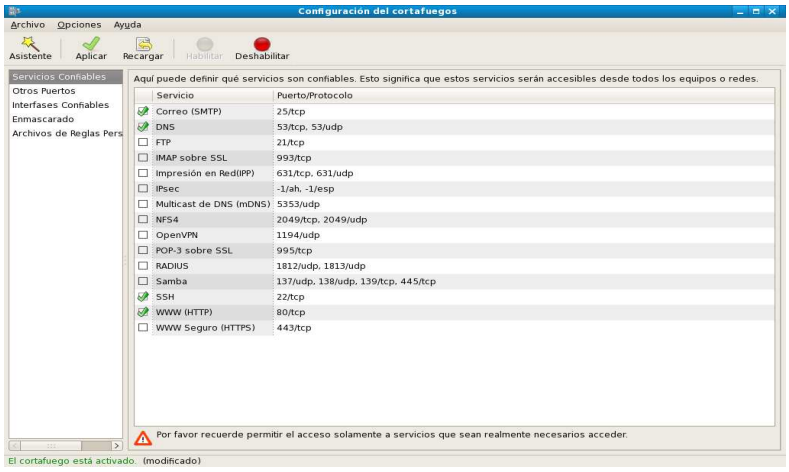


Figura3. 10: Configuración de los Iptables

7. Para aumentar los puertos que no vienen definidos por defecto ir a la opción otros puertos y añadir los necesarios en este caso Telnet puerto 23

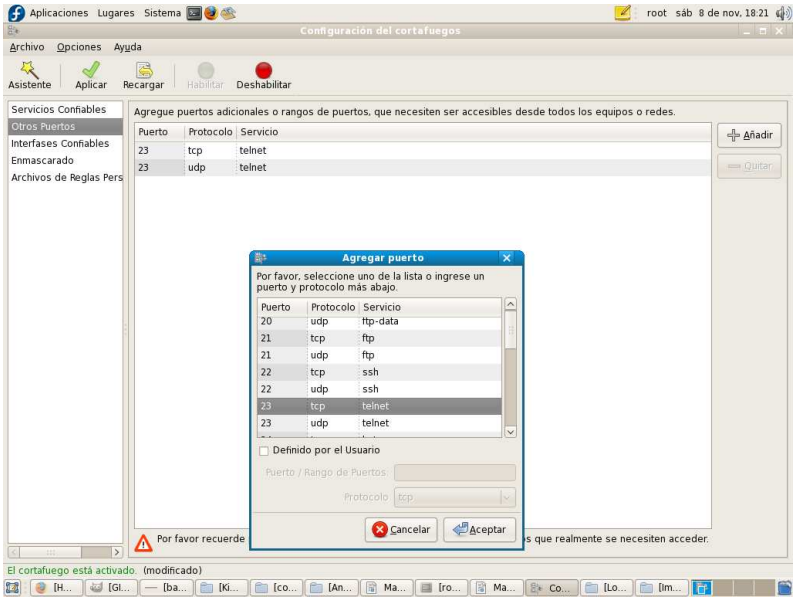


Figura3. 11: Agregar puertos necesarios como Telnet

3.5 Pruebas del Sistema de Honeypots

En la figura 3.12 se puede observar el resumen de los diferentes flujos de entrada y salida tanto de las interfaces internas como externas.

En la parte roja se observa que se generó una alerta de un ataque propiciado desde la interfaz externa.

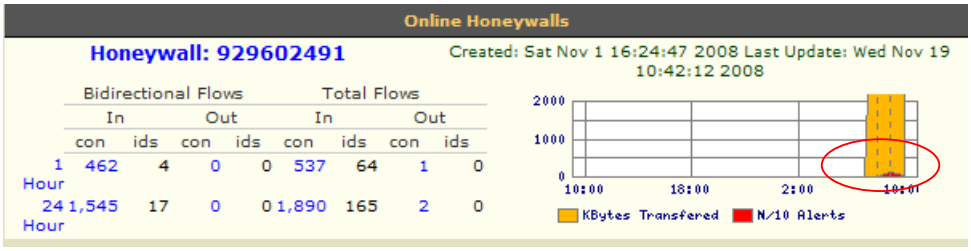


Figura3. 12: Flujos de entrada y salida de las interfaces internas y externas

En el registro de las alertas se puede ubicar en la alerta que se dio en el sistema de detección de intrusos, revisando la información desde donde se originó el ataque y el destino del mismo, realizando un clic en la dirección ip de destino del ataque se verifica desde donde se originó el mismo como se puede observar en la siguiente grafica.

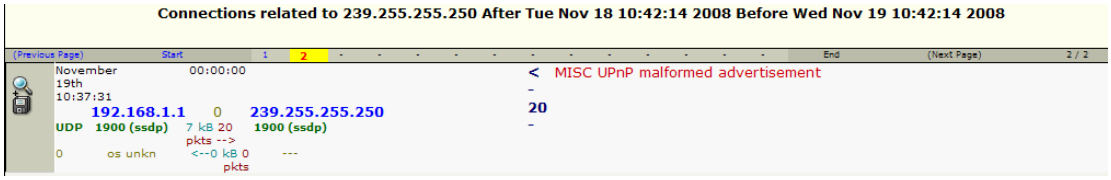


Figura3. 13: Alerta emitida por el sistema de detección de intrusos.

Figura3. 14: Información de la Ip que realizo la intrusión.

Otra de las pruebas importantes que se realizan para probar la funcionalidad de los sistemas Honeypots de baja interacción es saber que realizó el atacante dentro del sistema para lo cual utilizamos al paquete SEBEK con lo cual se tiene la siguiente figura.

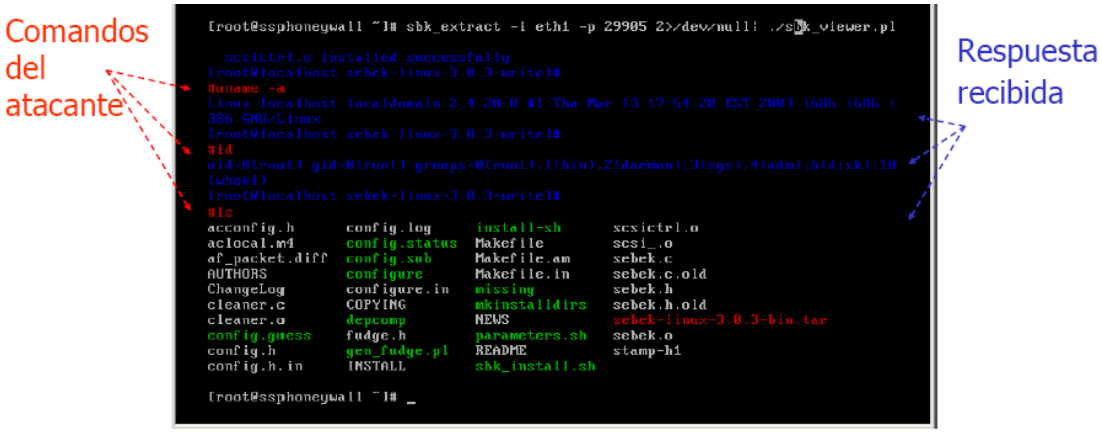


Figura3. 15: Despliegue de la información capturada del paquete Sebek.

Como se observó en la primera línea se realiza el extracto de lo acontecido dentro de la interfaz eth1 tomando como referencia la alarma que se generó de los paquetes recibidos por parte del IDS.

En la siguiente figura 3.16 se muestra el camino que el atacante realizó y los procesos involucrados dentro del ataque, lo cual permite determinar con mayor claridad que procesos son vulnerables dentro de la red.

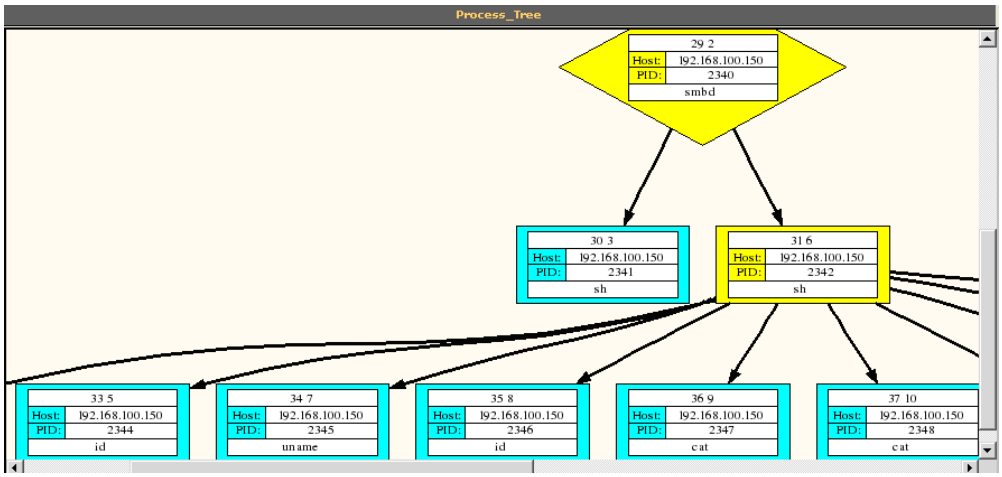


Figura3. 16: Árbol de procesos que realizo el atacante

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Se desarrollaron pruebas con un sistema de Honeypot, simulando un mecanismo de ataque para el ingreso al sistema en producción pero en realidad se dió el acceso al sistema de honeypots para ser analizado, detectado y puesto en una lista de posibles atacantes, y así se determinó que es un intruso de cuidado para la red de datos.

- El diseño del prototipo del sistema de honeypots permitió desarrollar un objeto de pruebas para la demostración de control de datos y el registro de administración remota de acceso a los mismos, como base para estudios posteriores que pueden servir de investigación y avances tecnológicos en el país.

- Mediante las pruebas que se realizaron se pudo analizar las diferentes medidas que se pueden tomar para proteger la red de datos y así prevenir los ataques maliciosos y controlarlos mediante un sistema de Honeypots, manteniendo el historial de la monitorización de conexiones entrantes y salientes, ficheros de configuración, y demás información relevante de los procesos que se controlaron durante la amenaza, que nos servirán como

patrones de prevención en la elaboración de la planificación del área de Tecnología de Información de cualquier organización.

- Los sistemas de honeypots son una interesante herramienta de seguridad y protección de la información; y a pesar de que no colaboran en la prevención directa de ataques, son un instrumento eficaz de reacción para la protección frente a estas amenazas. Y al ser considerado como Open Source y Código Abierto puede ser utilizado en exitosas investigaciones tecnológicas.

4.2 Recomendaciones

- Para iniciar el camino de actualización tecnológica dentro del país, sería apropiado que las empresas que buscan el éxito realicen una Planificación de Tecnologías de Información que contemple pruebas con un sistema de Honeypot, simulando un mecanismo de ataque, y redireccionando estas posibles amenazas hacia dicho sistema, para que sea considerado dentro de los posibles peligros que la organización debe tomar en cuenta y controlarlos y con ello buscar mejores herramientas para proteger su red lógica y física de datos.

- Se debe incentivar a los nuevos profesionales informáticos sobre la importancia de los estándares de seguridad informática y procesos

relacionados con el funcionamiento de la red física de las empresas, y el control de calidad dentro de tecnología de información, que garanticen el correcto y óptimo desempeño de todos los recursos.

- Es necesario que la planificación operativa de tecnología de información establezca parámetros de control de seguridad de la información con algunas de las normas o estándares existentes como: ISO 17799, 27001, RFC2196, OECD, ITSEC que me permitan implementar honeypots acorde a las necesidades institucionales.

- La preparación tecnológica del equipo que tiene la obligación de brindar protección y seguridad informática a la red será fundamental en la implementación de cualquier proyecto, implementando nuevas tecnologías que permitan retroalimentar la construcción en este caso de honeypot o cualquier otro tipo de herramienta especializada para la red de datos, y del ámbito de negocio de la empresa y de los datos que se necesite proteger de esta manera aseguramos el control del dominio a los posibles intrusos y por tanto las vulnerabilidades de la red.

- Una gran oportunidad para afrontar la competitividad latinoamericana en cuanto avances tecnológicos es utilizar herramientas de distribución libre, en las que se busque el acoplamiento a la funcionalidad de lo que requiere la organización y se pueda modificar el código fuente para que se ajuste de

mejor manera a las necesidades del honeypots y a la interacción que se le proporcione a la red de datos.

GLOSARIO DE TÉRMINOS

ACID: En bases de datos se denomina ACID a un conjunto de características necesarias para que una serie de instrucciones puedan ser consideradas como una transacción. Esto quiere decir que el mismo cuenta con las funcionalidades necesarias para que sus transacciones tengan las características ACID.

CGI: Es una tecnología que se usa en los servidores Web.

CÓDIGO ABIERTO: Es el término con el que se conoce al software distribuido y desarrollado libremente.

DATAGRAMA: Es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el equipo terminal de datos receptor, de manera independiente a los fragmentos restantes

DDOS: E un tipo especial de DoS consistente en la realización de un ataque conjunto y coordinado entre varios equipos (que pueden ser cientos o decenas de miles) hacia un servidor víctima.

DoS: Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos

FINGER: Es un protocolo del sistema operativo Linux que proporciona información de los usuarios de una máquina que estén o no conectados en el momento de acceder al servicio.

FTP: Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red.

GATEWAY: Es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

HIPERTEXTO: Es el texto que en la pantalla de una computadora conduce a su usuario a otro texto relacionado.

HOSTNAME: Es un nombre único que se le da a un dispositivo conectado a una red informática.

HTML: Es el lenguaje de marcado predominante para la construcción de páginas Web.

INTERNET: Es un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolo TCP/IP.

LAN: Una red de área local, o red local, es la interconexión de varios ordenadores y periféricos. (*LAN* es la abreviatura inglesa de *Local Area Network).* Su aplicación

más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

LENGUAJE DE MARCADO: Es una forma de codificar un documento que, junto con el texto, incorpora etiquetas o marcas que contienen información adicional acerca de la estructura del texto o su presentación.

LOG: Es un registro oficial de eventos durante un periodo de tiempo en particular.

NIDS: Es un sistema de detección de intrusos en una Red. Busca detectar anomalías que inicien un riesgo potencial, tales como ataques de denegación de servicio, escaneadores de puertos o intentos de entrar en un ordenador, analizando el tráfico en la red en tiempo real.

NMAP: Es un programa de código abierto que sirve para efectuar rastreo de puertos TCP/IP y UDP.

PROTOCOLO: Es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red.

REDES DE COMUNICACIÓN: Es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos

(CD-ROOM, impresoras, etc.) y servicios (acceso a Internet, e-mail, chat, juegos), etc.

SNIFFERS: Es un aplicación de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.

TCPDUMP: Es un herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red.

TCP/IP: Es un protocolo el cual es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa.

UDP: Es un protocolo del nivel de transporte dentro del modelo OSI basado en el intercambio de datagramas.

UNIX: Es un sistema operativo de tiempo compartido, controla los recursos de una computadora y los asigna entre los usuarios. Permite a los usuarios correr sus programas. Controla los dispositivos de periféricos conectados a la máquina.

WAN: Una red de área amplia o WAN (Wide Area Network) se extiende sobre un área geográfica extensa, a veces un país o un continente, y su función

fundamental está orientada a la interconexión de redes o equipos terminales que se encuentran ubicados a grandes distancias entre sí.

WEBSITE: Es un conjunto de paginas Web, típicamente comunes a un dominio de Internet o subdominio en la Web en Internet. Una página Web es un documento HTML/XHTML accesible generalmente mediante el protocolo HTTP de Internet.

WORLD WIDE WEB: Es un sistema de documentos de hipertexto y/o hipermedios enlazados y accesibles a través de Internet.

XHTML: Es el lenguaje de marcado lenguaje de marcado pensado para sustituir a HTML como estándar para las páginas Web.

BIBLIOGRAFÍA

- http://www.mike.com.mx/UAT_Honeypots.pdf
- http://www.honeynet.org.mx/es/
- http://www.software.net.mx/desarrolladores/softwareprofesional/seguridad/Honeynetproject.htm
- http://www.honeynet.org.mx/es/data/files/Papers/UAT_Honeypots_ES.pdf
- http://www.honeynet.ec
- http://www.google.com.ec
- http://www.wikipedia.org/
- http://his.sourceforge.net/trad/honeynet/
- http://www.snort.org/
- http://www.honeyd.org
- http://www.tracking-hackers.com
- http://www.tcpdump.org
- www.slideshare.net/gppoloc/protocolos-y-modelo-osi/
- www.monografias.com/trabajos29/modelo-osi/modelo-osi.shtml
- es.wikipedia.org/wiki/TCP/IP
- www.honeynet.org/tools/sebek/
- www.todo-linux.com/
- www.honeynet.unam.mx/
- www.honeypots.net/honeypots/products
- honeypots.sourceforge.net/

ANEXO A

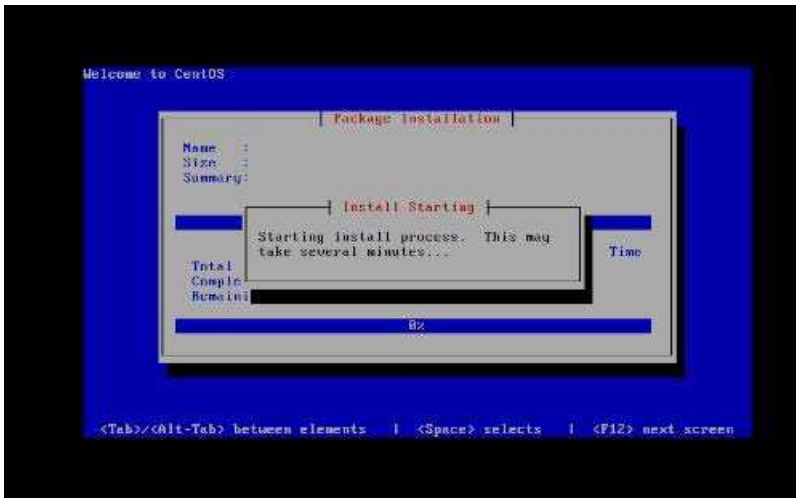
Instalación y Configuración del ROO 1.4 (Honeywall)

FORMATO: roo-1.4.hw-20080424215740.iso.

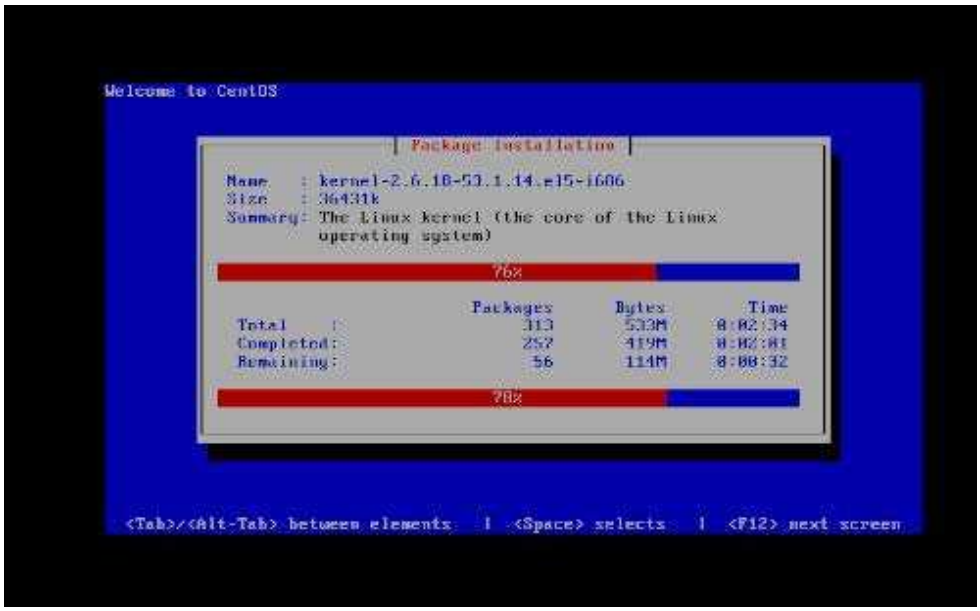
1. Inserte el CD y presione la tecla Enter.

FiguraA. 1: Inicio de Instalación

2. Proceso de instalación de los paquetes.



FiguraA. 2: Pantalla Instalación de Paquetes



FiguraA. 3: Pantalla de transcurso de instalación

3. Interfaz de configuración del Honeywall.

FiguraA. 4: Configuración del Honeywall

4. Interfaz de carga del Kernel

FiguraA. 5: Carga del Kernel

5. Ingreso del login y password

FiguraA. 6: Ingreso Login y Password

INGRESAR COMO ROOT

localhost login: roo

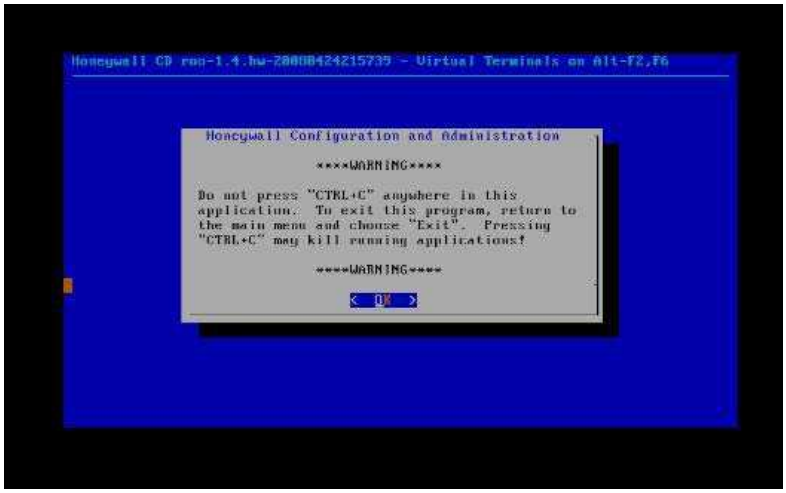
password: demonio

[root@localhost ~] $ su –

password: 123456

FiguraA. 7: Interfaz de acceso como ROOT

6. Para iniciar con la configuración del Honeywall presione la tecla Enter:



FiguraA. 8: Interfaz de configuración del Honeywall

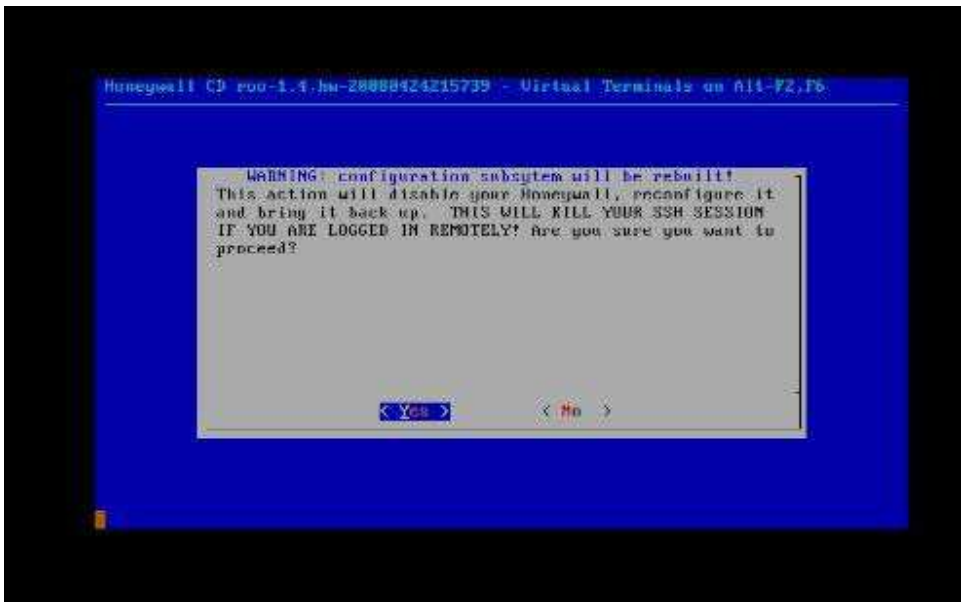
7. Seleccionar Honeywall Configuration.

FiguraA. 9: Selección de Honeywall Configuration

8. Seleccionar Reconfigure system

FiguraA. 10: Selección de Reconfiguración del Sistema

9. Aceptar Warning: configuration subsystem will be rebuilt



FiguraA. 11: Pantalla de confirmación Warning

10. Seleccionar Interview, y luego presionar Enter:

FiguraA. 12: Selección de Interview

11. Leer "Know your enemy: Honeynets" y presionar Enter:

FiguraA. 13: Pantalla de “Know your enemy: Honeynets”

12. Escribir la dirección IP para su honeypot y posteriormente presionar Enter

FiguraA. 14: Ingreso de IP del Honeynet

13. Escriba la red que va a ser utilizada para la Honeynet.

FiguraA. 15: Pantalla de ingreso de la Red Honeynet

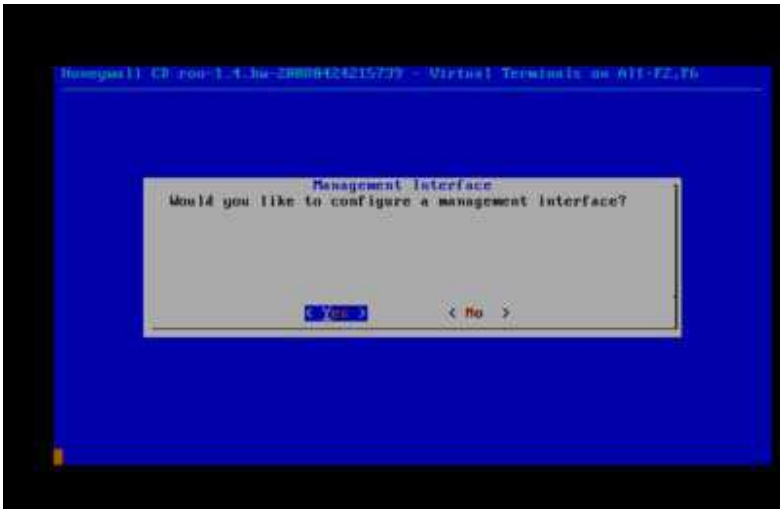
14. Presione la tecla Enter

FiguraA. 16: Inicialización del Setup

15. Ingrese la dirección de broadcast y luego presione la tecla Enter:

FiguraA. 17: Interfaz de ingreso de la dirección de Broadcast

16. Presione Ok y luego Enter



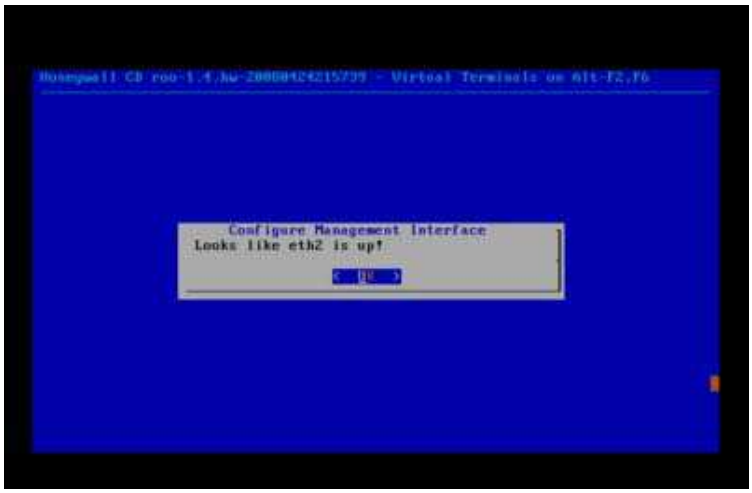
FiguraA. 18: Administración de Interfaz

Mediante la opción de Management Interface permite realizar la Administración Remota del Honeywall a través del SSH y de la interfaz web del Walleye.

17. Honeywall detecta automáticamente la interfaz de administración para la Eth2. Presionar Enter para continuar.

FiguraA. 19: Administración de la Interfaz Eth2

18. Presiona la tecla Enter:

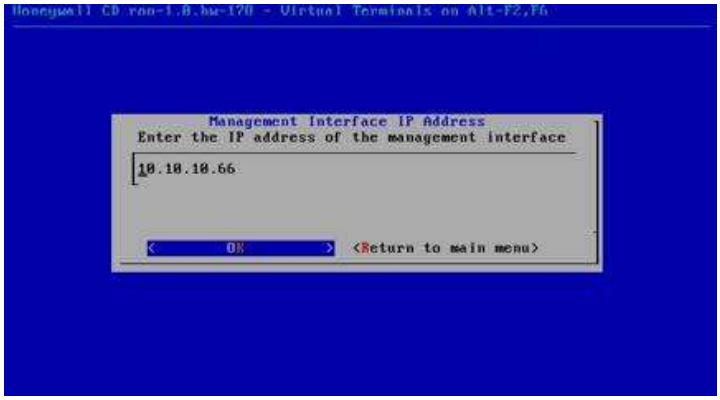


FiguraA. 20: Configuración de la Administración de la interfaz

Ingrese la dirección IP de la interface de administración: Esta es la dirección IP de la 3ra interfaz de la tarjeta de red. Se podrá conectar a esta dirección para

ingresar al sitio web de la administración del Honeywall. Este sitio web permitirá controlar la Honeywall y revisar la actividad de la red.

19. Presione la tecla Enter:

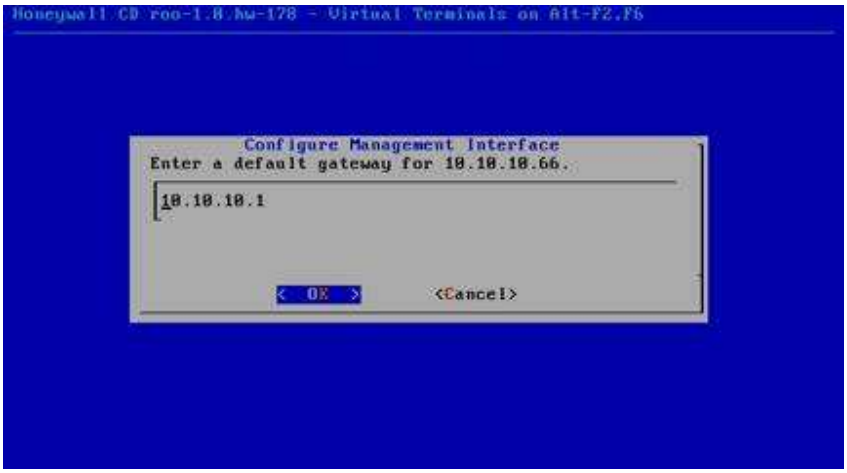


FiguraA. 21: IP de control del Honeywall

20. Presione la tecla Enter:

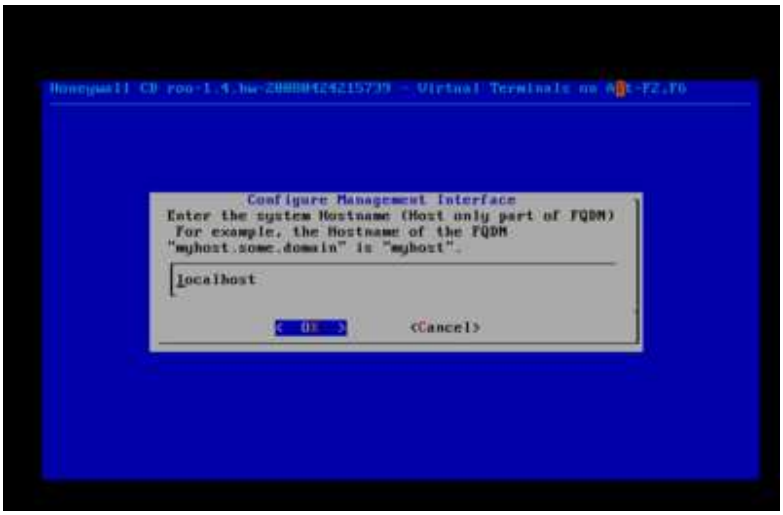
FiguraA. 22: Configuración de la máscara de red

21. Ingrese una default gateway para la interfaz de administración y luego presione la tecla Enter.



FiguraA. 23: Ingreso de Gateway de la interfaz de administración

22. Interfaz de personalización de nombre del Honeywall. Presione la tecla Enter:



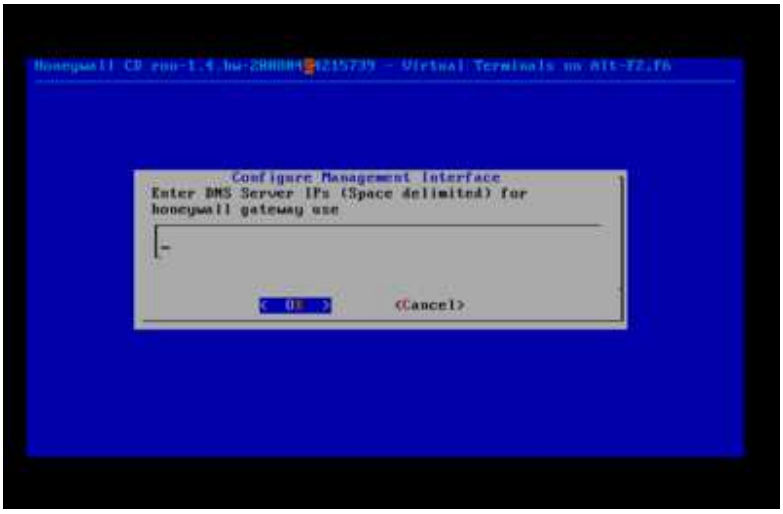
FiguraA. 24: Personalización de nombre del Honeywall

23. Presione la tecla Enter:

FiguraA. 25: Nombre del localdomain

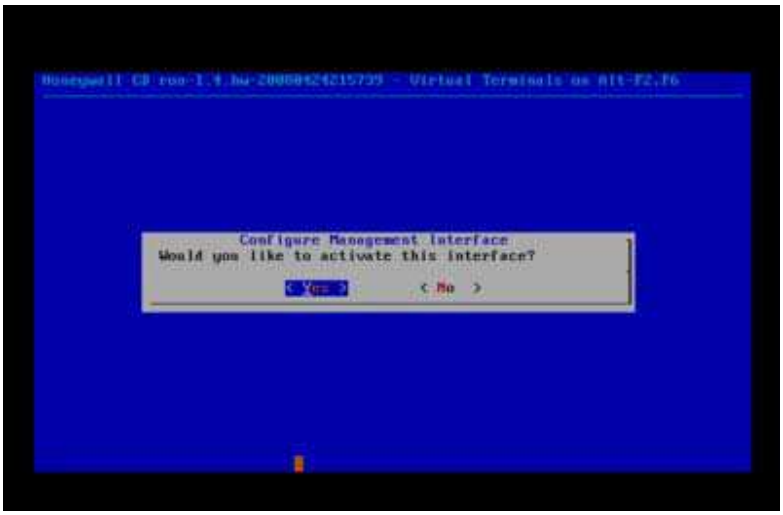
Ingresar las ***direcciones IPs de los servidores DNS***. Si usted tiene más de una dirección de servidor DNS ingresar un espacio entre las direcciones, finalmente la tecla Enter:

24. Ingresar la dirección IP del DNS y presionar OK (ejemplo 10.0.0.1)



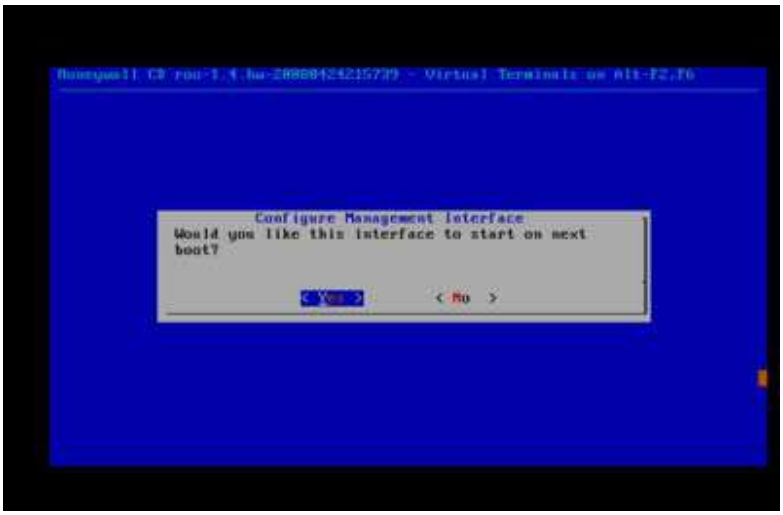
FiguraA. 26: Ingreso de dirección IP del DNS

25. Seleccione Yes y presione la tecla Enter



FiguraA. 27: Confirmación de la configuración de la interfaz

26. Seleccione Yes y presione la tecla Enter:

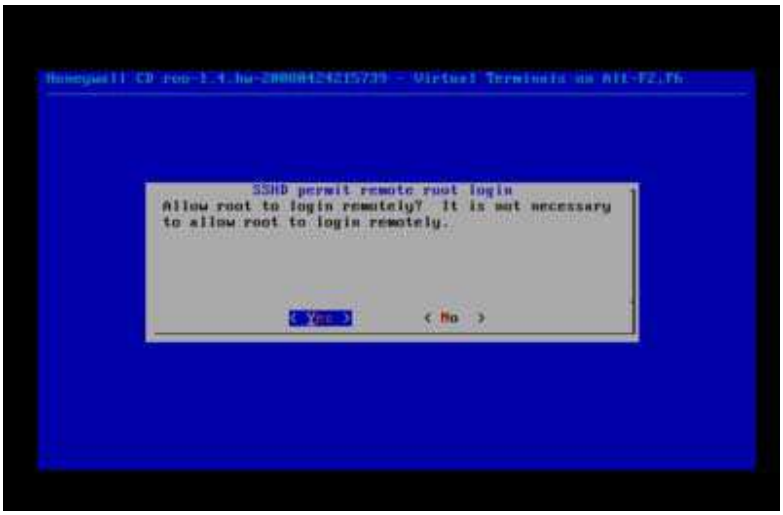


FiguraA. 28: Aceptar para iniciar

27. En la configuración del SSH por defecto se escucha en el puerto 22. Seleccione Yes y presione la tecla Enter:

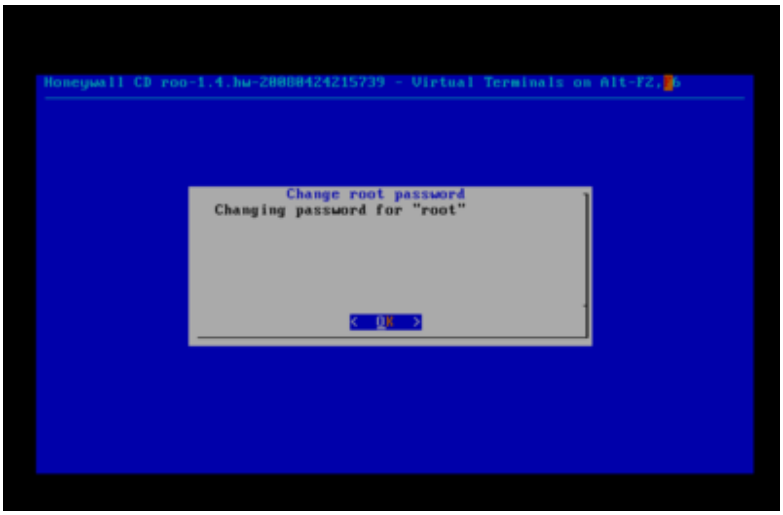
FiguraA. 29: Configuración del SSH

28. Seleccione Yes y presione la tecla Enter:



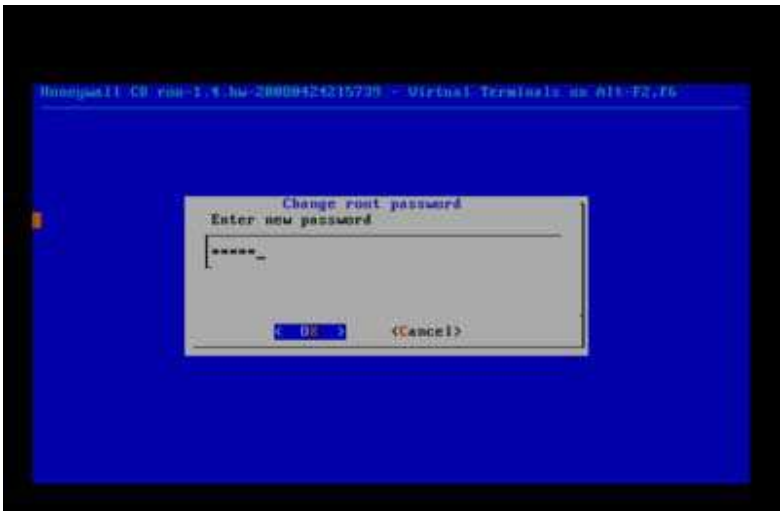
FiguraA. 30: Permiso de Acceso Remoto

29. Presione la tecla Enter:



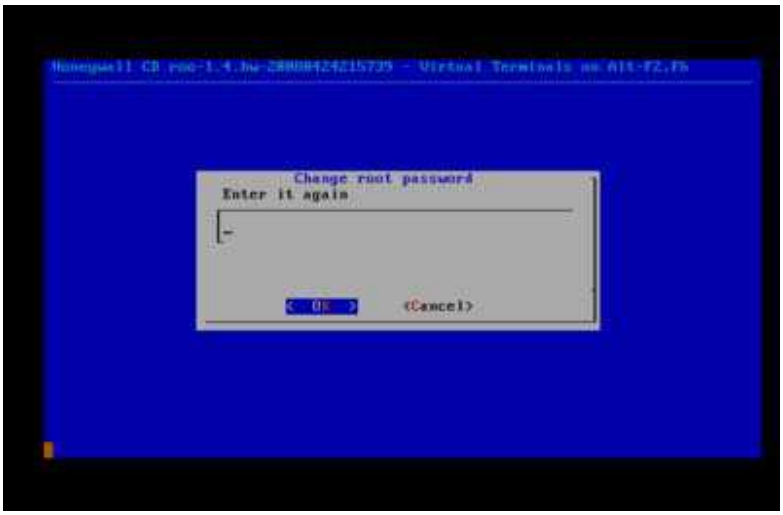
FiguraA. 31: Cambio de contraseña del Root

30. Crear una contraseña para root (Se recomienda 14 o mas caracteres), y presione la tecla Enter:



FiguraA. 32: Ingreso de contraseña

31. Confirmar la contraseña de root y presionar la tecla Enter:

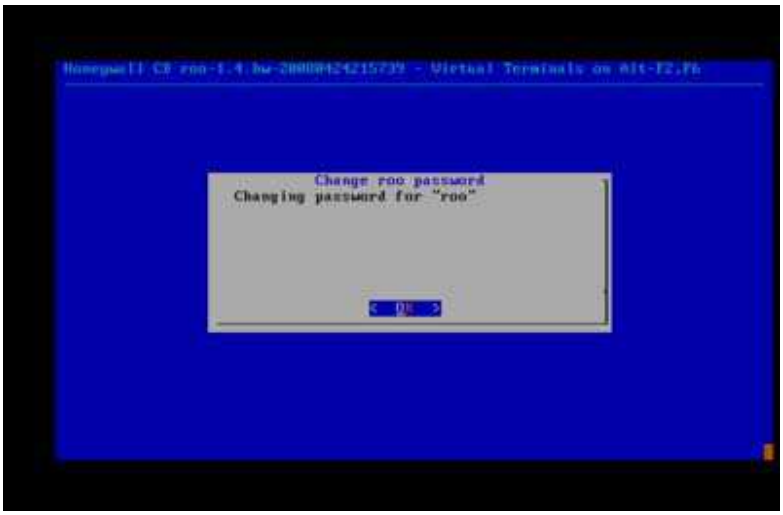


FiguraA. 33: Confirmación de contraseña

32. Presione la tecla Enter:

FiguraA. 34: Clave cambiada

33. Presione la tecla Enter:



FiguraA. 35: Cambiar la clave del Roo

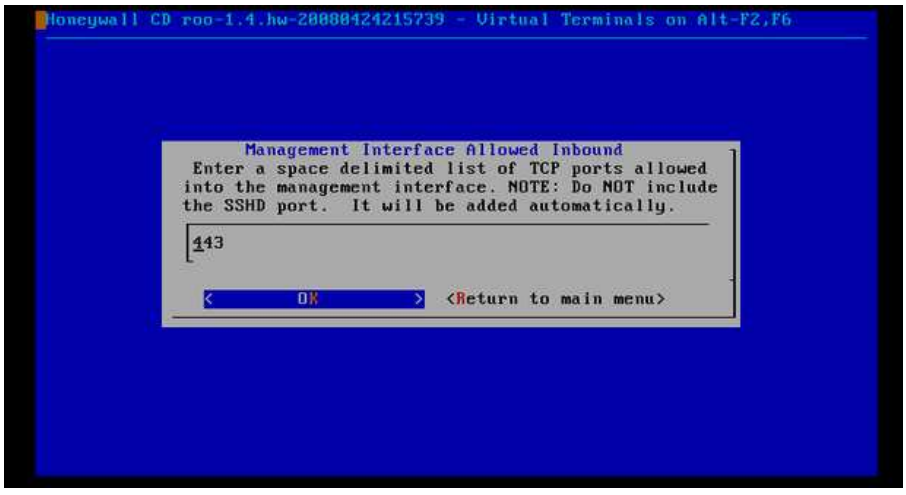
Repita la creación de la contraseña para el usuario consola del roo (línea de comando) y presione Enter:

FiguraA. 36: Ingreso de contraseña

34. Presione la tecla Enter:

FiguraA. 37: Confirmación de cambio de contraseña

El puerto 443 será usado con la encriptación SSL (https) al acceder a la administración web del Honeywall y luego presionar Enter:

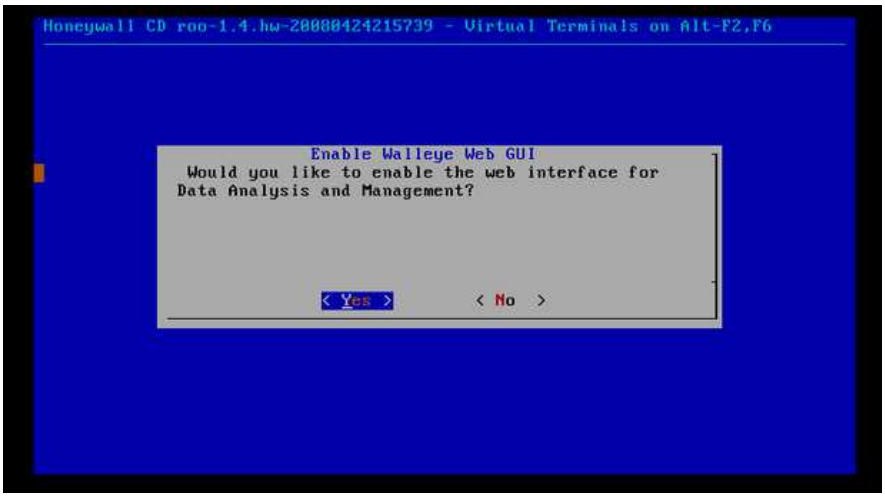


FiguraA. 38: Confirmación de puerto para encriptación SSL

35. Ingrese una dirección IP que permita conectar a la web de la administración de la Honeywall y presione Enter:

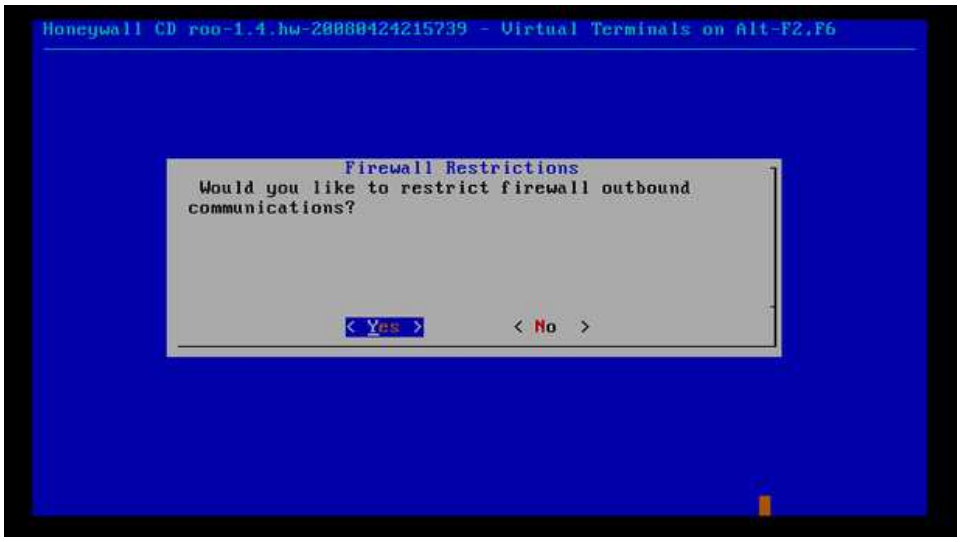
FiguraA. 39: IP para conexión a la Web de administración de la Honeywall

36. Presione la tecla Enter para habilitar la Interface Web:



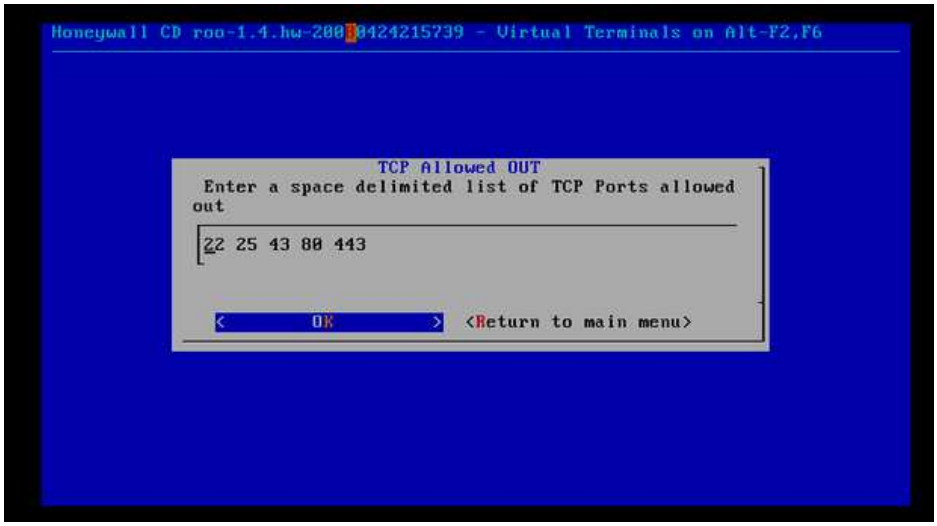
FiguraA. 40: Habilitar la interfaz Web

37. Firewall restrictions ayudara a prevenir troyanos y malware. Presione la tecla Enter:



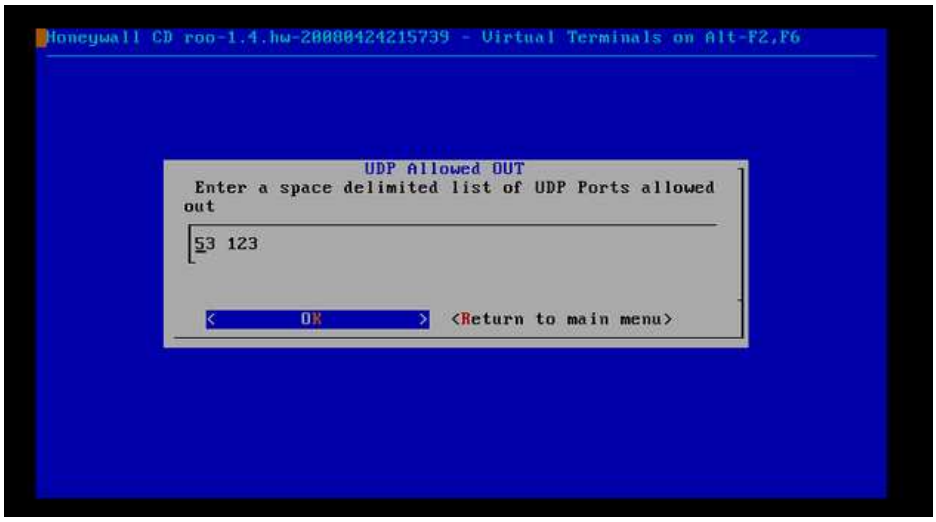
FiguraA. 41: Restricciones de Firewall

38. Ingrese la lista de puertos TCP necesarios separados por un espacio en blanco, y luego presione Enter:



FiguraA. 42: Ingreso de puertos TCP

39. Ingrese la lista de puertos UDP necesarios para la red separados por un espacio en blanco y luego presione la tecla Enter:



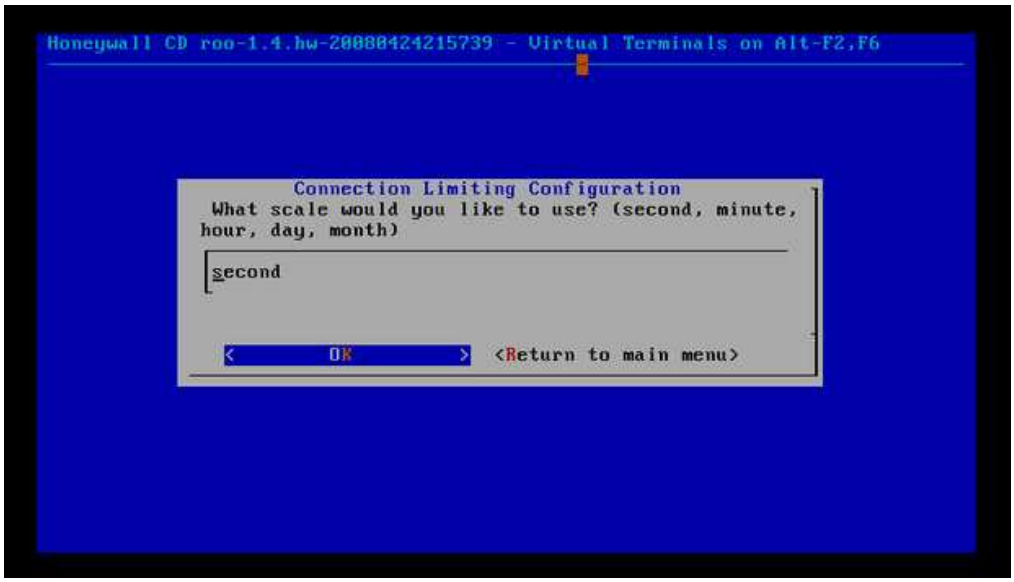
FiguraA. 43: Ingreso de puertos UDP

40. Presione la tecla Enter:

FiguraA. 44: Inicialización del Setup

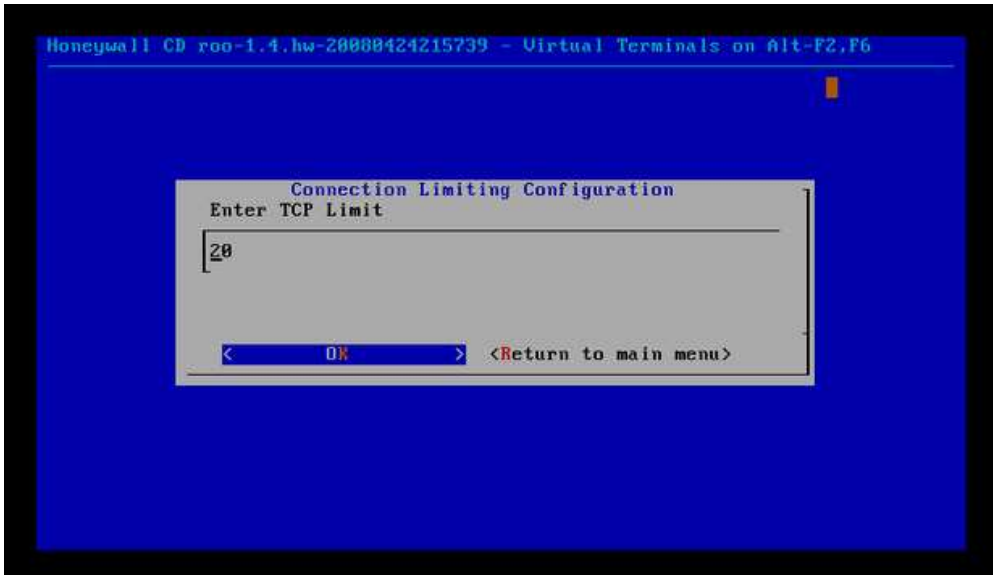
41. Opción que permite cambiar la escala a: segundo, minuto, hora, día o mes.

    Finalmente presione la tecla Enter:



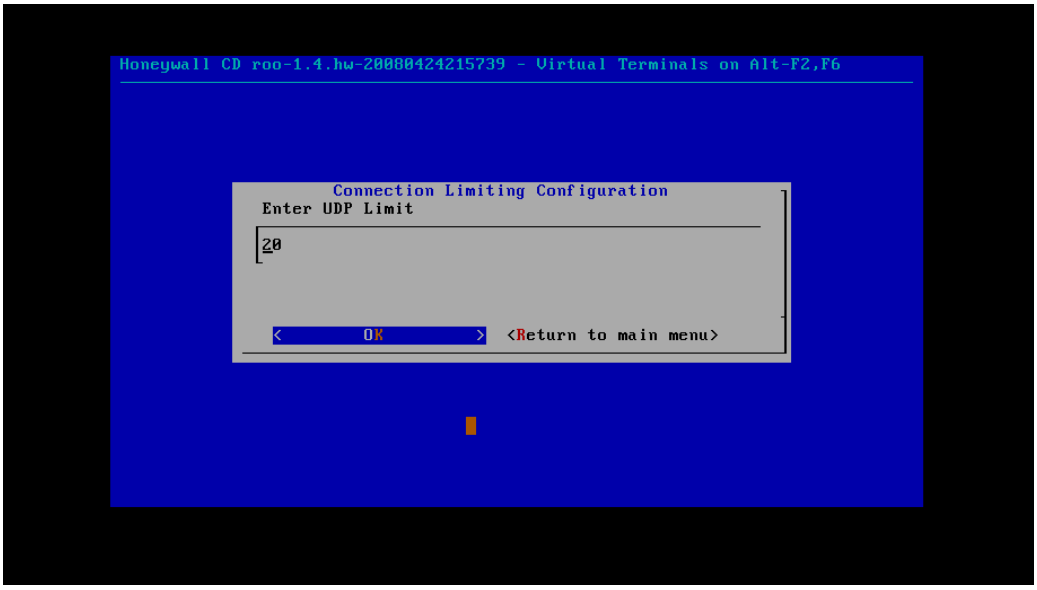
FiguraA. 45: Configuración de limite de conexiones

42. Muestra el limite de conexiones TCP y Presione la tecla Enter:



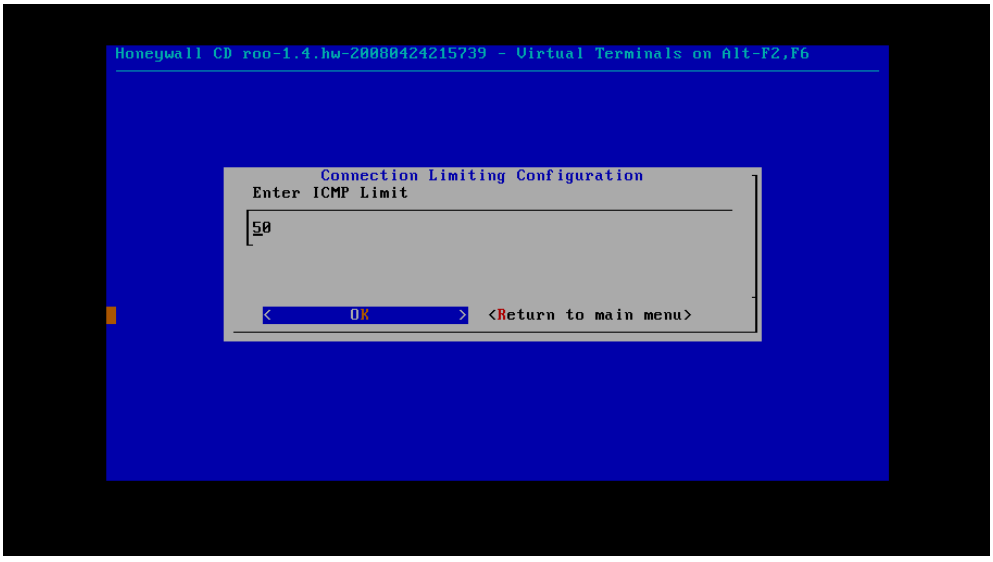
FiguraA. 46: Limite de conexiones TCP

43. Muestra el limite de conexiones UDP y presiones la tecla Enter:



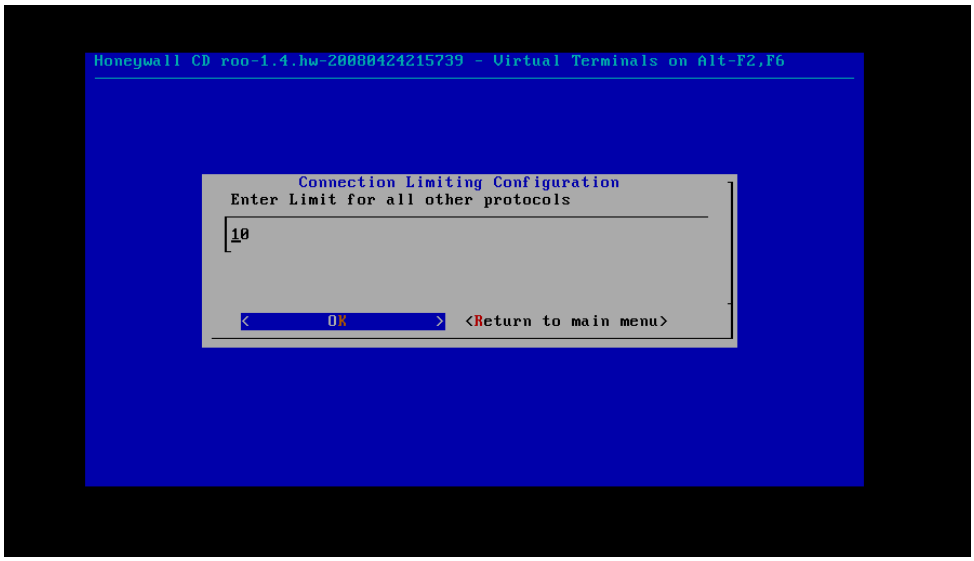
FiguraA. 47: Limite de Conexiones UDP

44. Muestra el limite de conexiones ICMP y presione la tecla Enter:



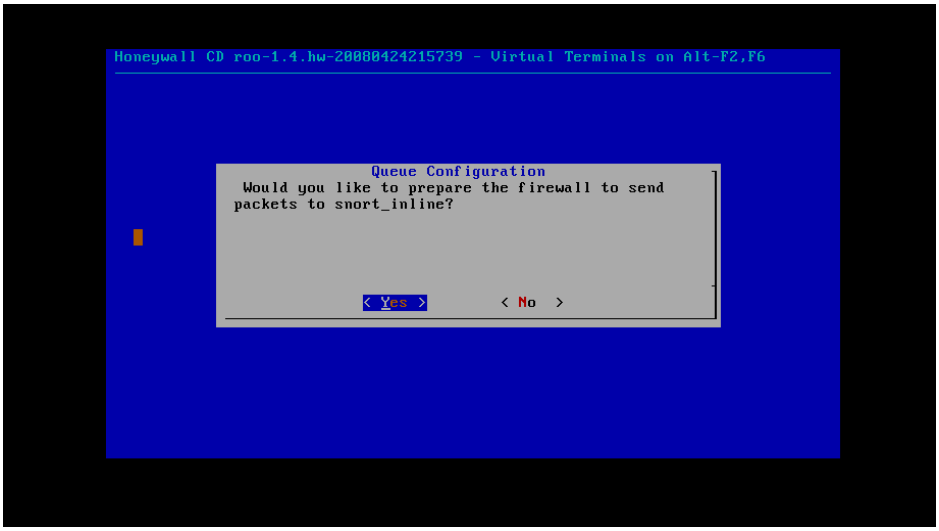
FiguraA. 48: Limite de conexiones ICMP

45. Muestre el limite de conexiones para otros protocolos y presione la tecla Enter:



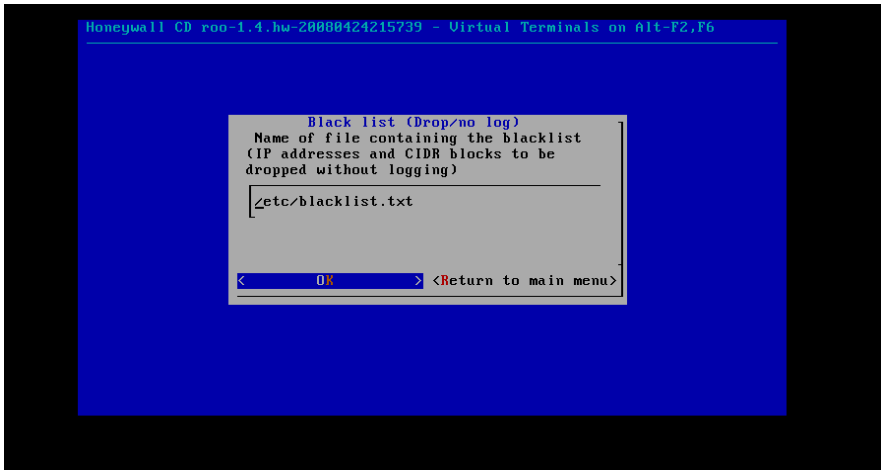
FiguraA. 49: Limite de conexiones para otros protocolos

46. Habilitar el snort-inline: Evita que el tráfico malicioso llegue a la red. Selecciones yes y presione la tecla Enter



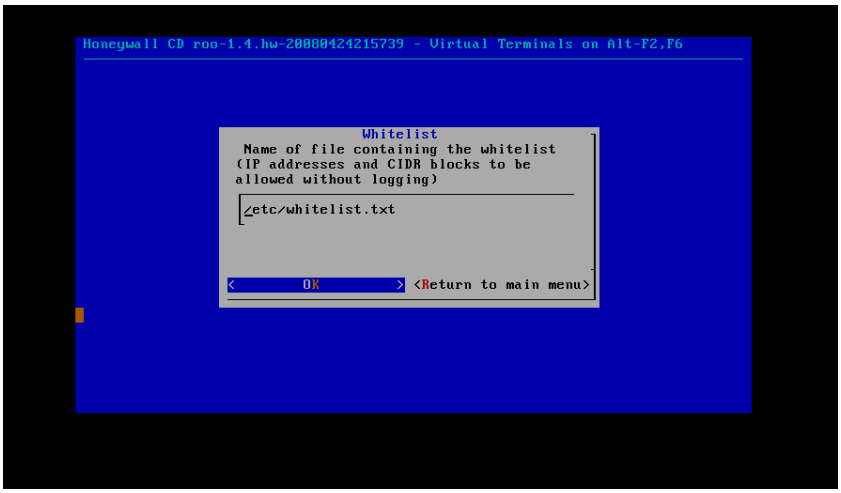
FiguraA. 50: Habilitar Snort-inline

47. Blacklist o lista negra es una lista donde se registran las direcciones IPs que generan spam de forma voluntaria o involuntaria. Seleccione OK y presione la tecla Enter



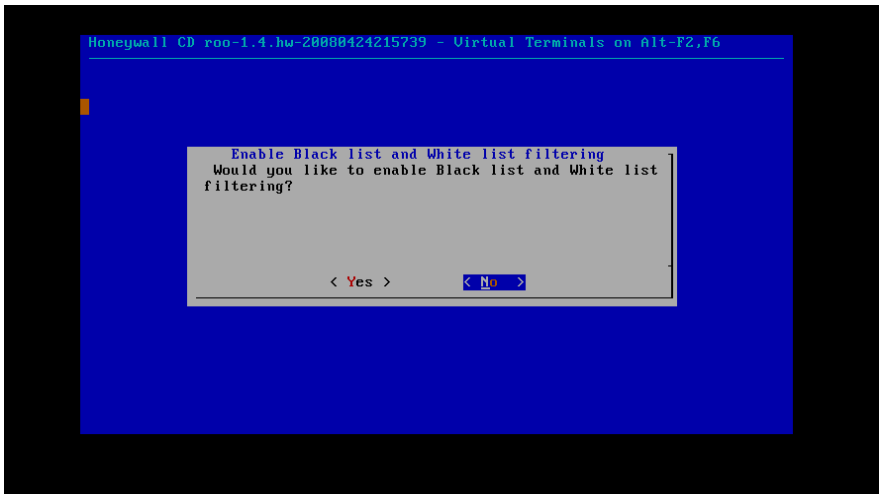
FiguraA. 51: Blacklist “registro de IPs de generación de Spam”

48. Whitelist o lista blanca, aquí se detalla la direcciones IPs fijadas por el usuario que nunca y bajo ningún concepto los mensajes provenientes de éstas deben ser detectadas y consideradas por el sistema como Spam. Presione Ok y presione la tecla Enter



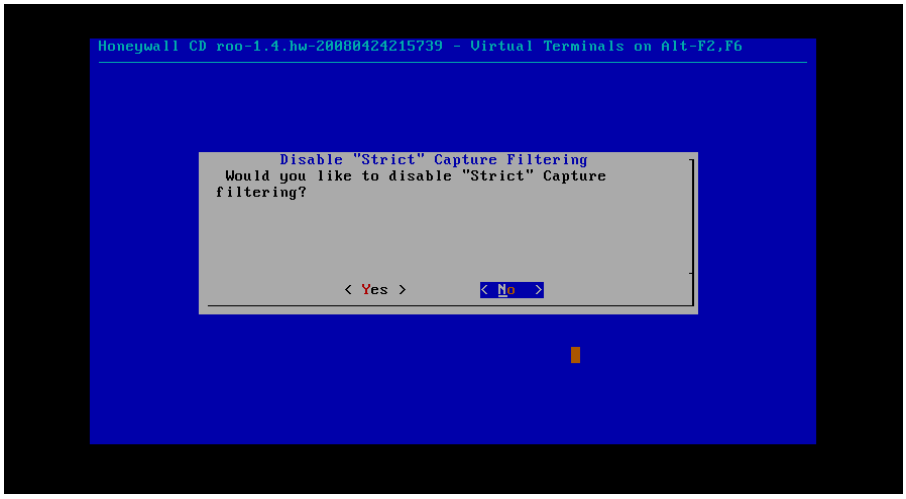
FiguraA. 52: Whitelist “IPs fijadas por el usuario”

49. Enable Black list and White list filtering: Seleccione Yes y presione la tecla Enter



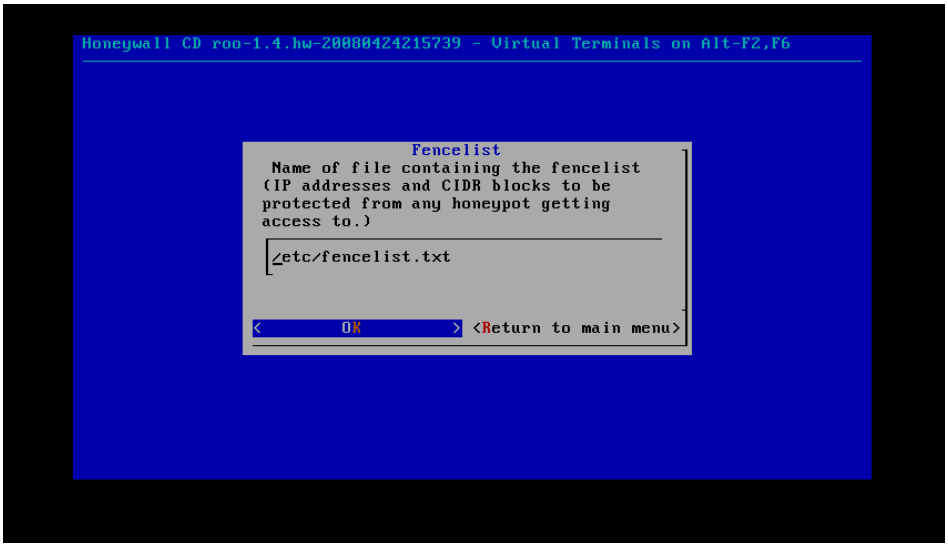
FiguraA. 53: Habilitar lista blanca y lista negra

50. Disable "Strict" Capture Filtering: Seleccione Yes y presione la tecla Enter



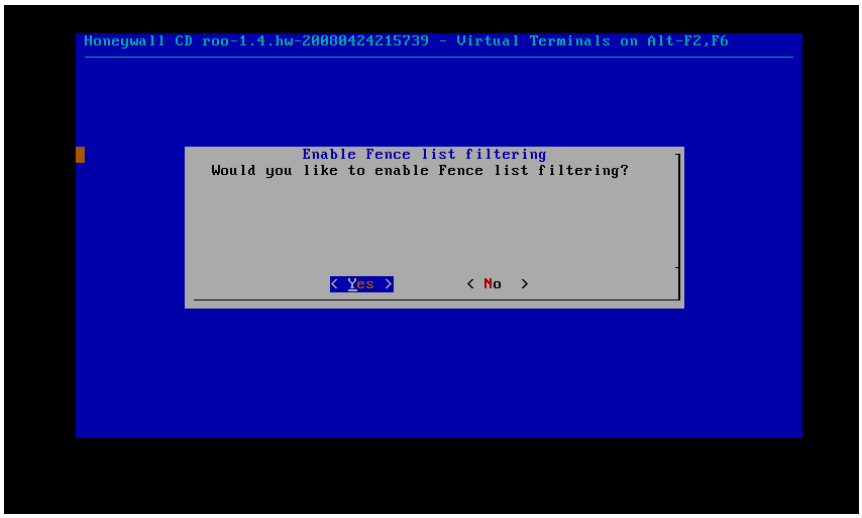
FiguraA. 54: Deshabilitar Strict capture filtering

51. Fencelist es la herramienta más importante para asegurar las redes de producción. Su aplicación crea reglas en el firewall que bloquee todo el tráfico a determinados objetivos. Seleccione Ok y presione la tecla Enter:



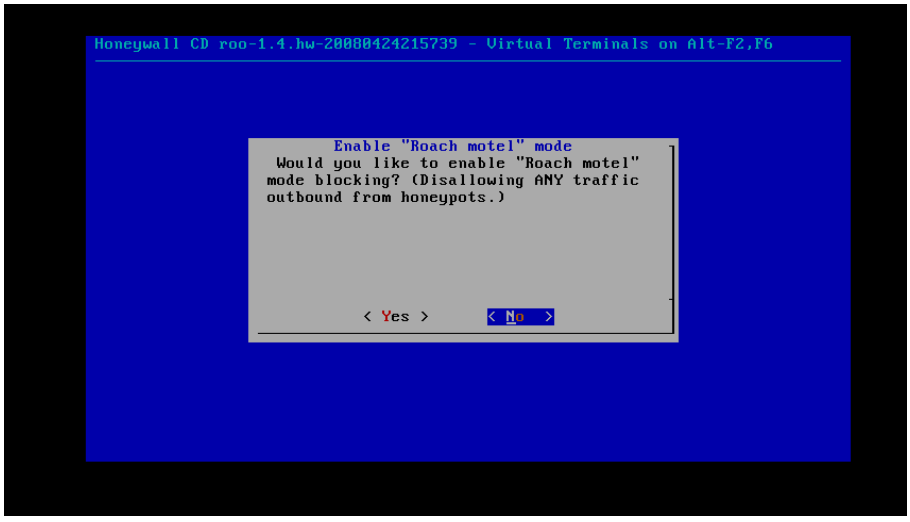
FiguraA. 55: Creación de reglas firewall mediante FENCELIST

52. Enable Fence list filtering: seleccione yes y presione la tecla Enter



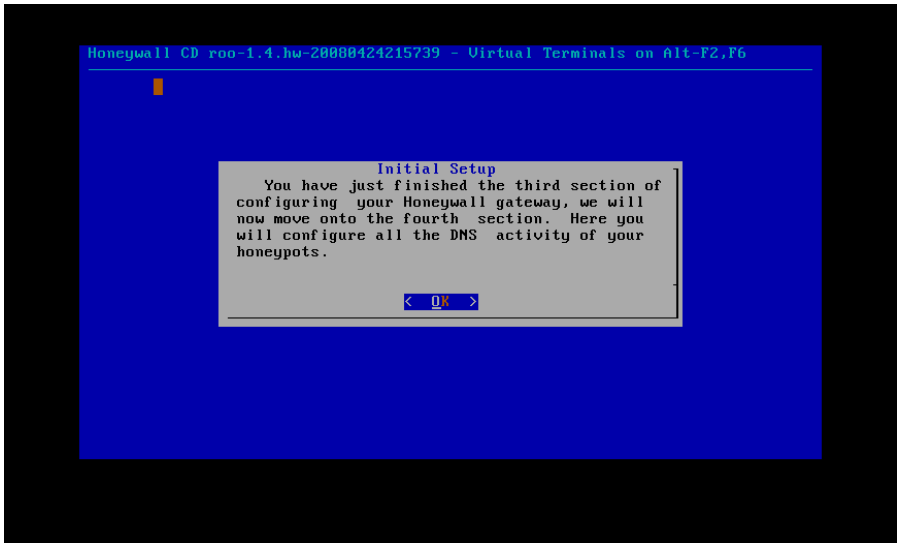
FiguraA. 56: Habilitar Fence list filtering

53. Roach motel mode: Si se habilita Roach motel mode, un atacante podría fácilmente detectar su Honeywall y posteriormente atacarlo, por eso es aconsejable desactivar el bloqueo de todo el tráfico saliente de honeypots. Seleccionar *No* y luego presionar la tecla *Enter*:



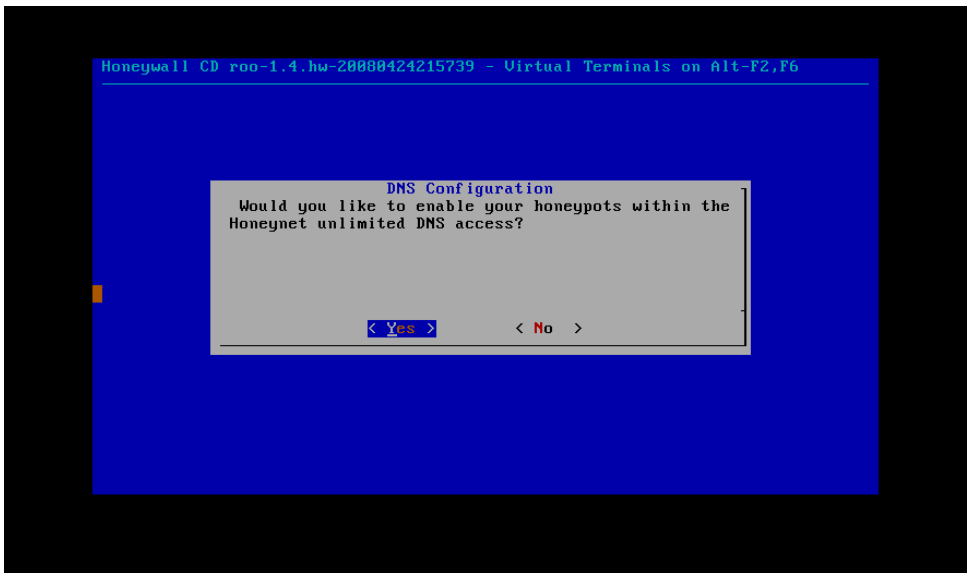
FiguraA. 57: Habilitar “Roach motel” mode

54. Presione la tecla Enter:



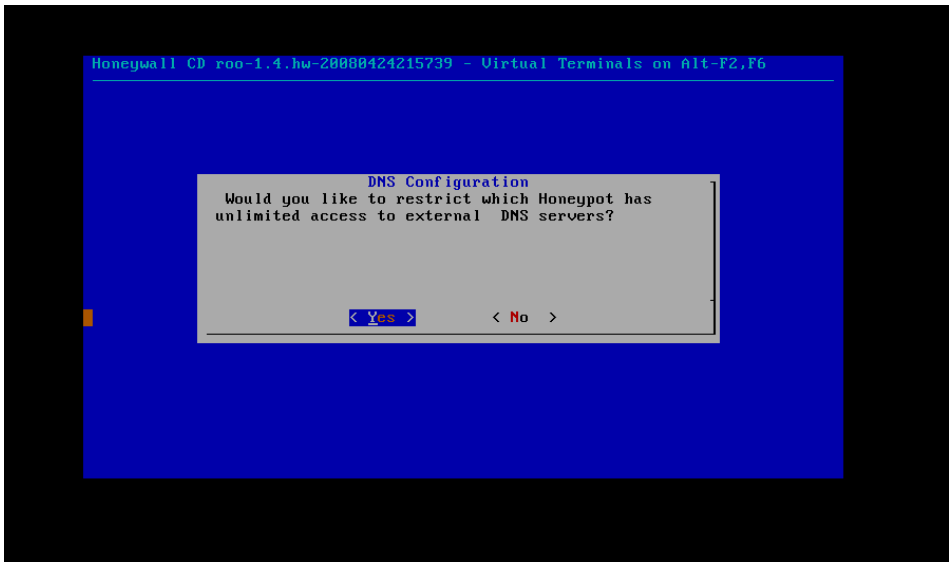
FiguraA. 58: Confirmación de configuraciones realizadas

55. Seleccione Yes y luego presione la tecla Enter:



FiguraA. 59: Configuración DNS del Honeywall

56. Seleccione Yes y presione la tecla Enter

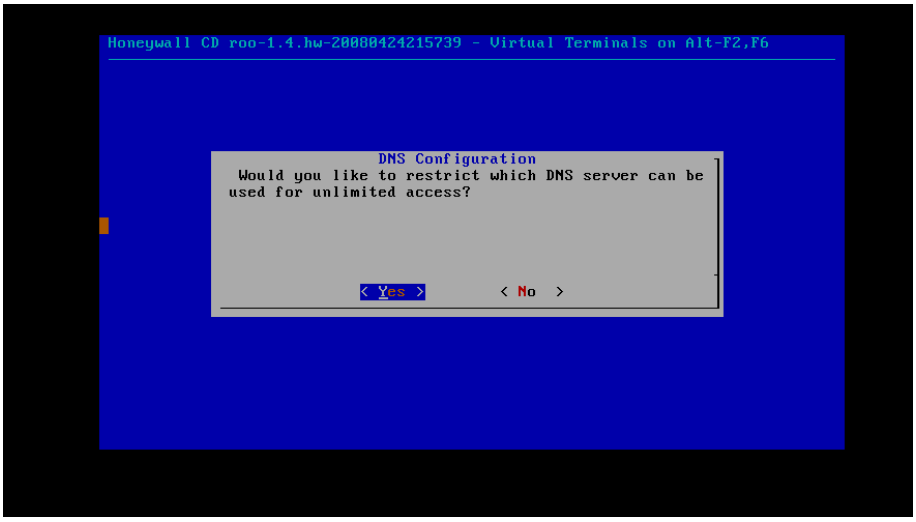


FiguraA. 60: Aceptación de la configuración del DNS

57. Ingrese la lista de los Honeypots seleccione OK y presione Enter

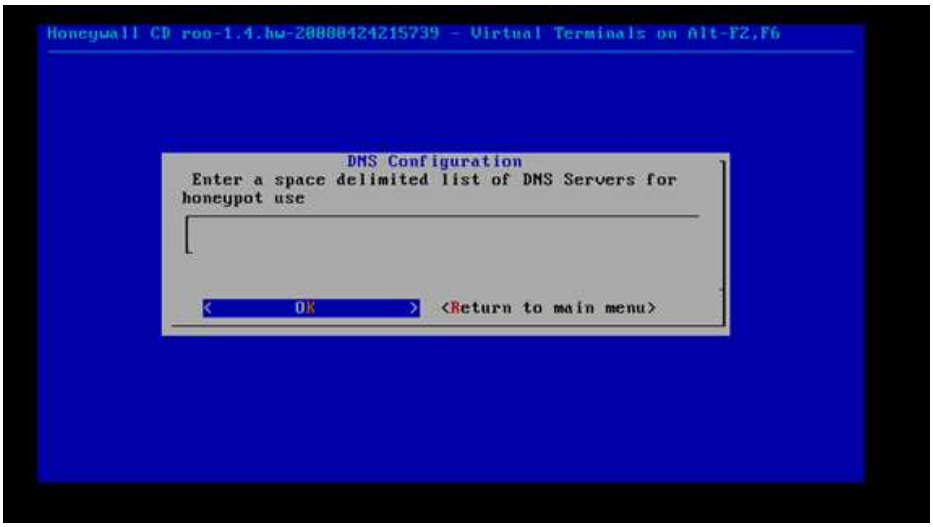
FiguraA. 61: Ingreso de lista Honeypots

58. Seleccione Yes y presione la tecla Enter



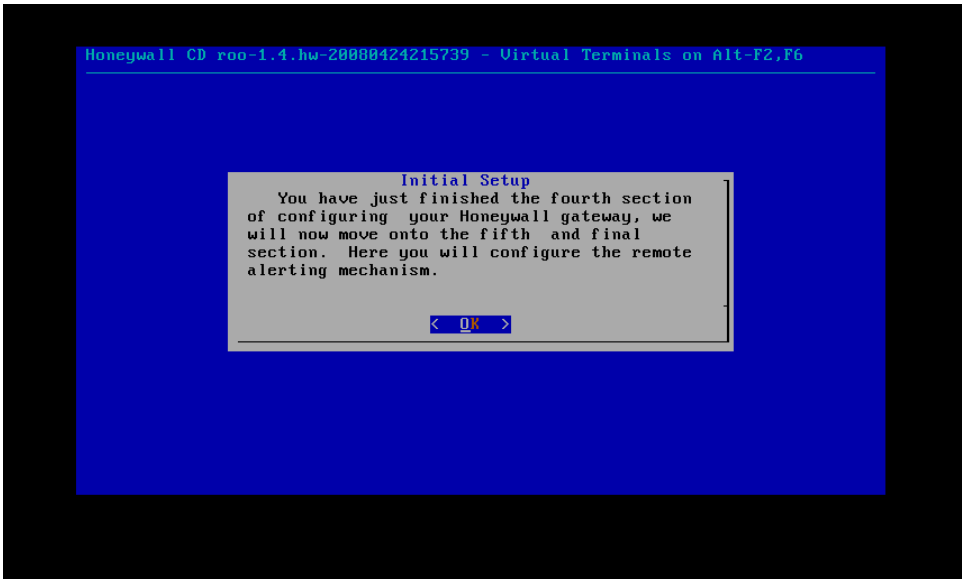
FiguraA. 62: Confirmación de lista Honeypots

59. Configuración DNS presione Enter



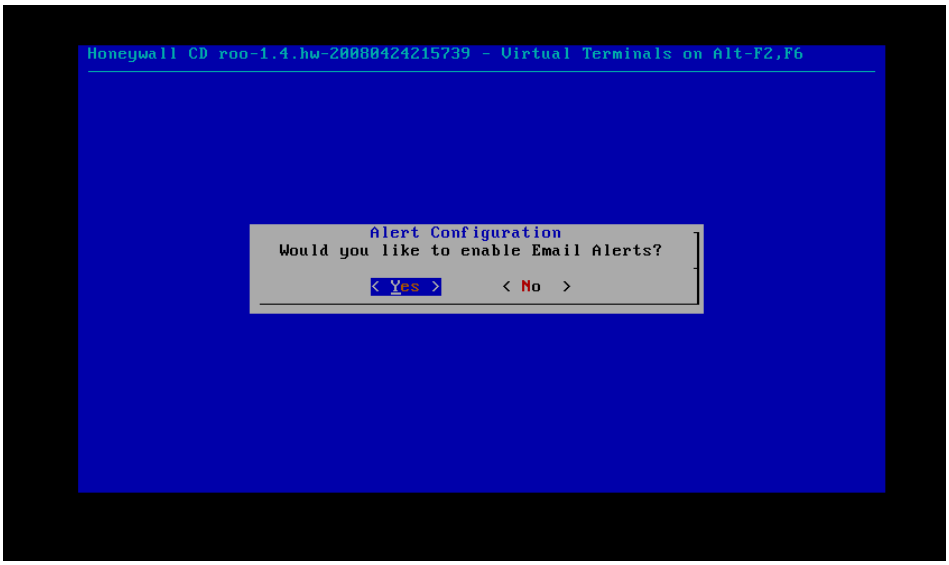
FiguraA. 63: Limite de lista de servidores DNS para Honeypot

60. Presione la tecla Enter:



FiguraA. 64: Confirmación de configuraciones DNS

61. Seleccione Yes y presione la tecla Enter

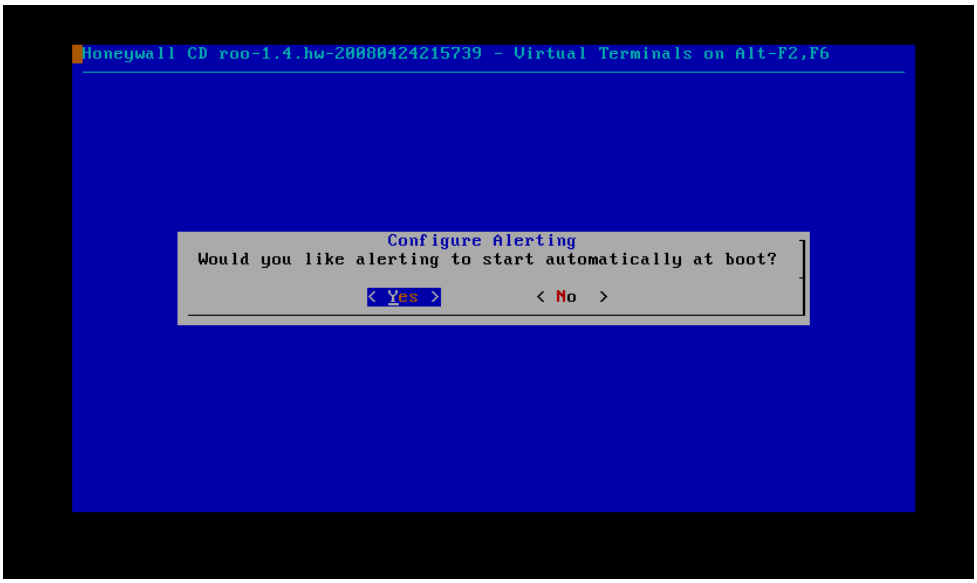


FiguraA. 65: Configuraciones de Alerta

62. Ingrese el correo electrónico deseado **root@localhost.localdomain** para recibir las alertas, seleccione Ok y presione Enter

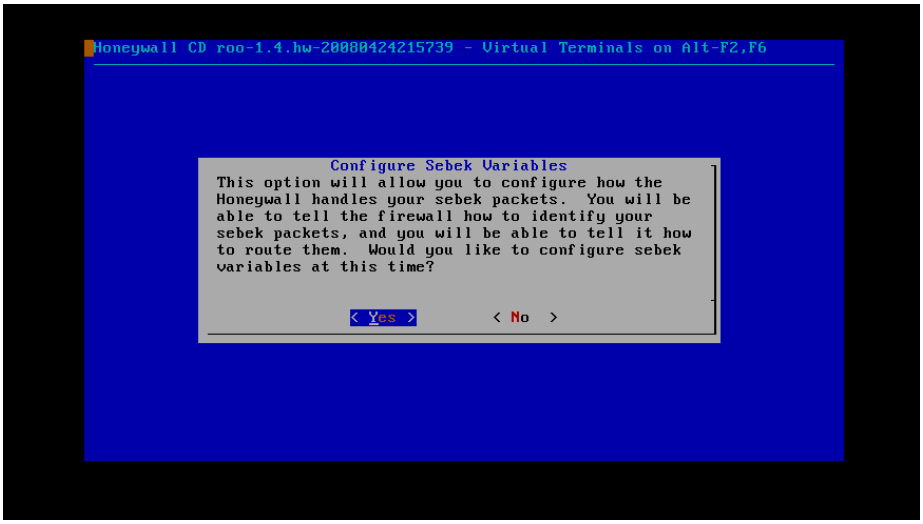
FiguraA. 66: Ingreso de correo electrónico para Alertas

63. Seleccione Yes y presione la tecla Enter



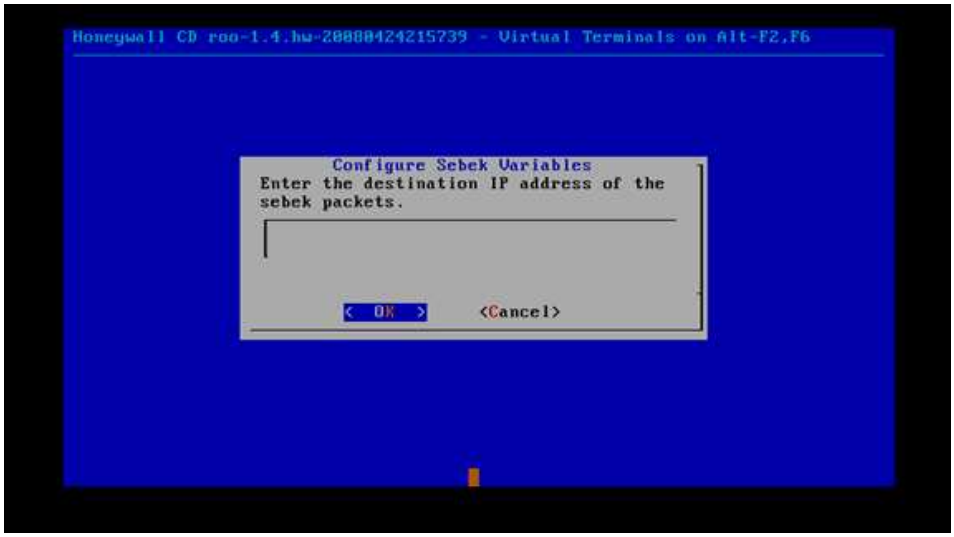
FiguraA. 67: Configuración de alertas automáticas

64. Seleccione Yes y presione la tecla Enter



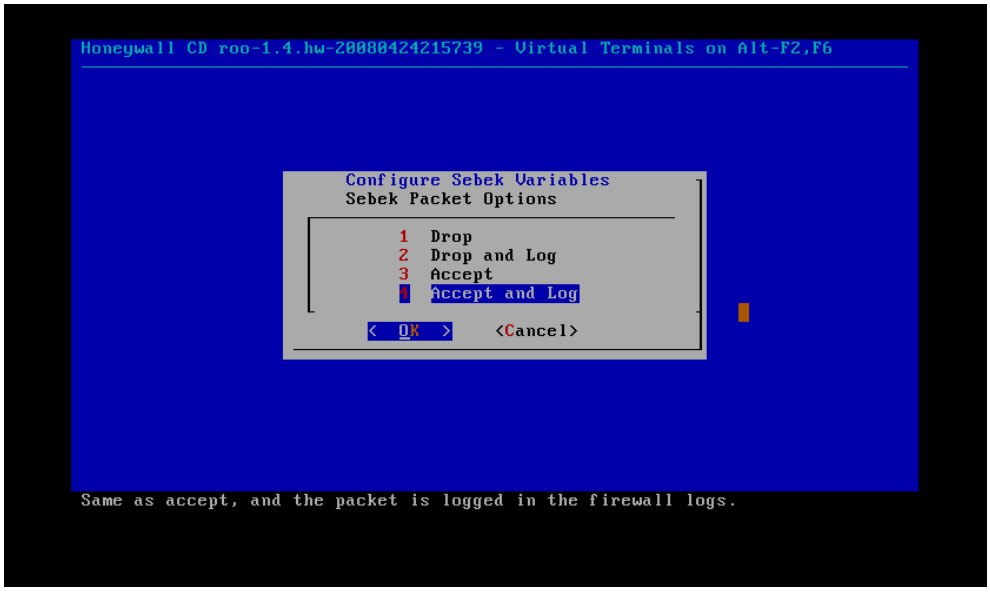
FiguraA. 68: Confirmación de configuraciones de alertas

65. Modifique la dirección IP destino de los paquetes del Sebek a otro Honeywall, o a otra dirección IP de la red de área local. Ingrese la dirección IP y luego presione la tecla Enter:



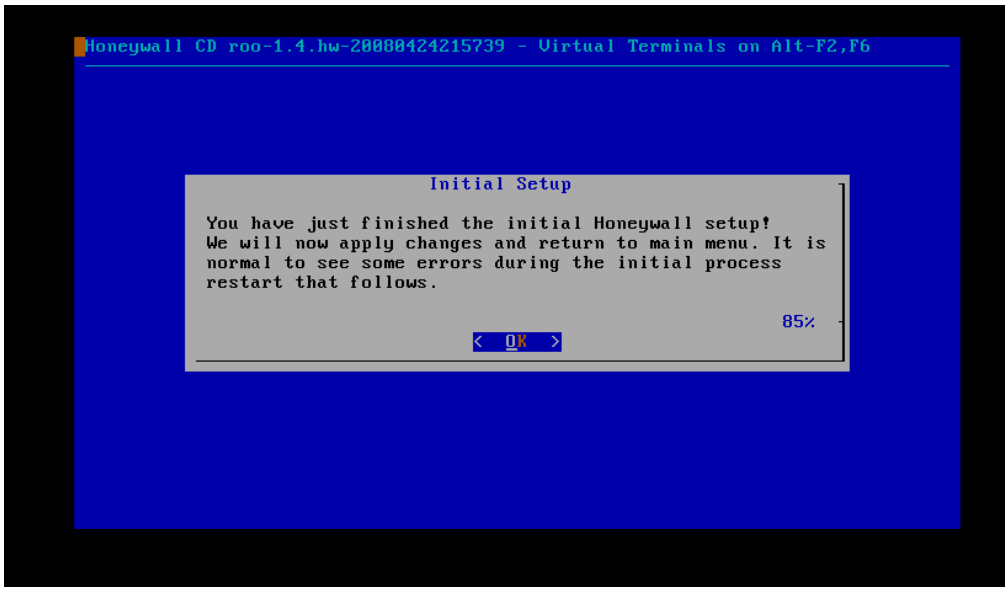
FiguraA. 69: Modificación de IP de paquetes SEBEK

66. Seleccionar Accept and Log



FiguraA. 70: Selección de Accept and Log

67. Presione la tecla Enter:

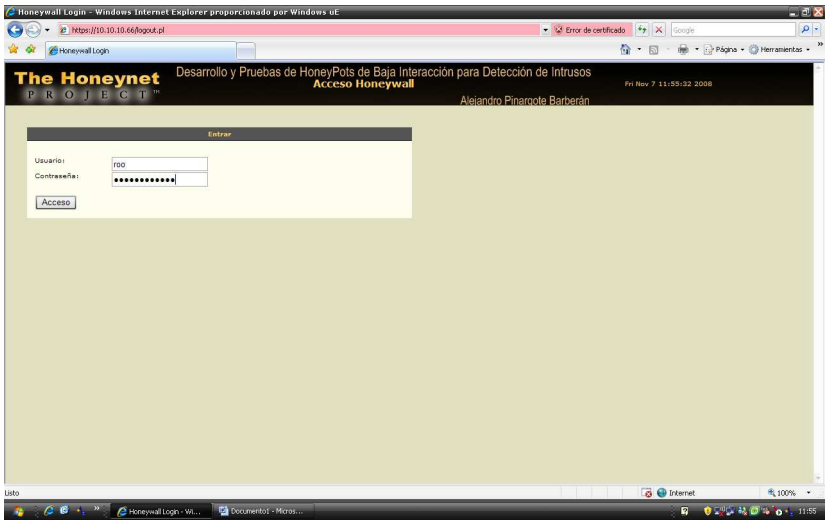


FiguraA. 71: Confirmación de configuraciones

ANEXO B

1. ACCESO AL HONEYWALL

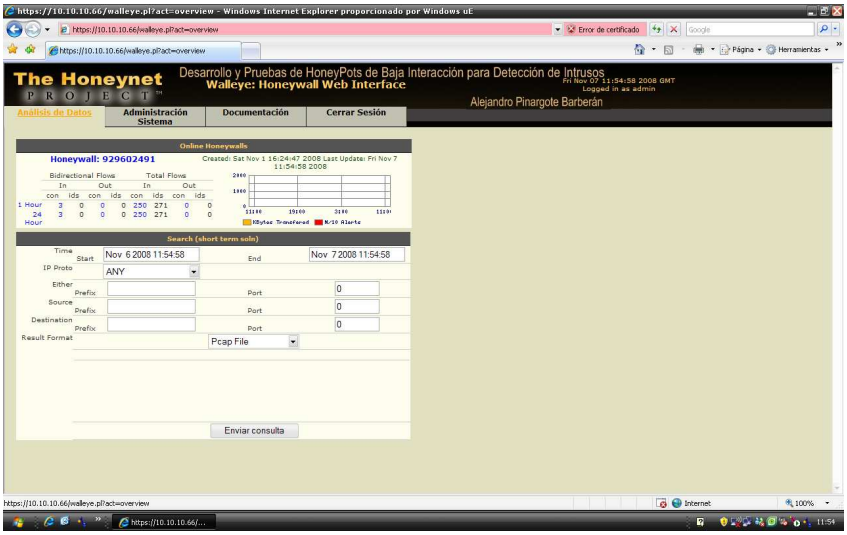
Interfaz Web de acceso a Honeywall



FiguraB. 1: Acceso al Honeywall

2. ANÁLISIS DE DATOS

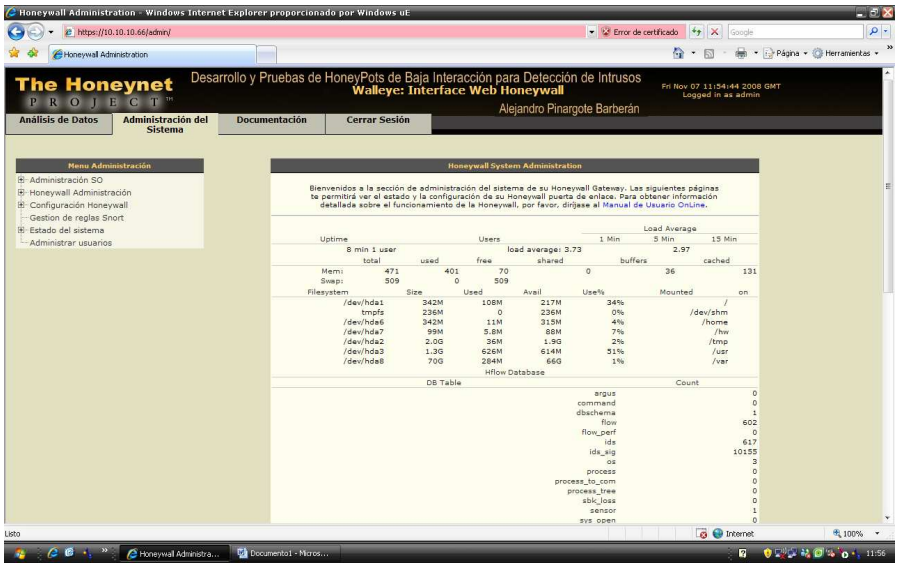
Despliegue de datos sobre control de trafico, puertos y datos del intruso.



FiguraB. 2: Análisis de Datos

3. ADMINISTRACIÓN DEL SISTEMA OPERATIVO

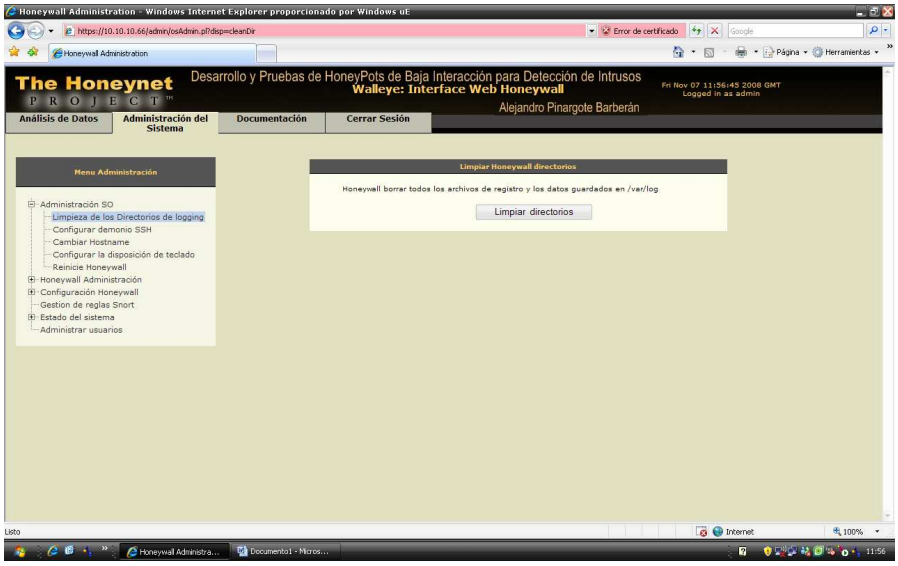
Interfaz donde se visualiza el estado y la configuración del Honeywall



FiguraB. 3: Administración del Sistema Operativo

4. LIMPIEZA DE LOS DIRECTORIOS DE LOGGING

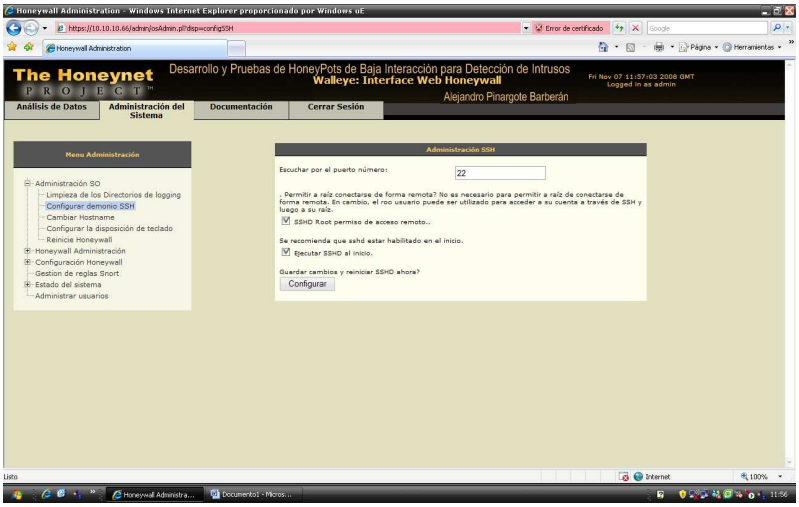
Permite borrar los archivos de registro que tenemos almacenados y los datos guardados en /var/log.



FiguraB. 4: Limpieza de los Directorios de Logging

5. CONFIGURAR DEMONIO SSH

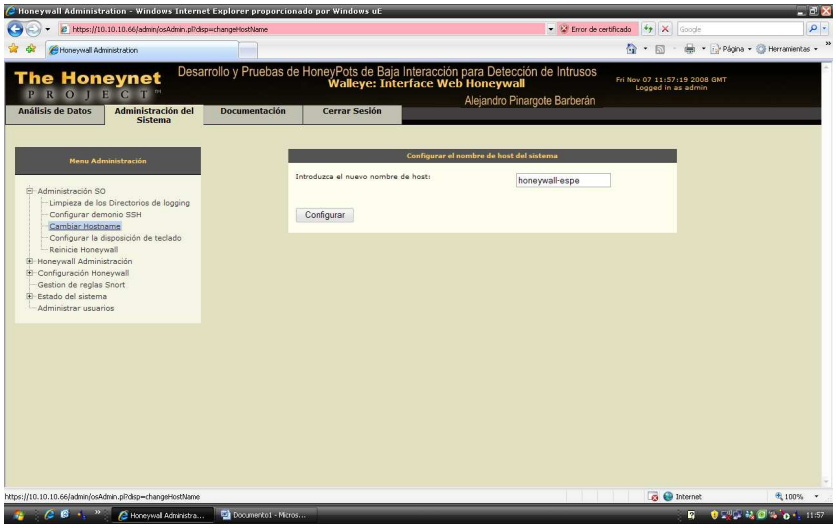
Interfaz de configuración del demonio SSH para acceder de forma remota y por defecto escucha en el puerto 22.



FiguraB. 5: Configuración Demonio SSH

6. CAMBIAR HOSTNAME

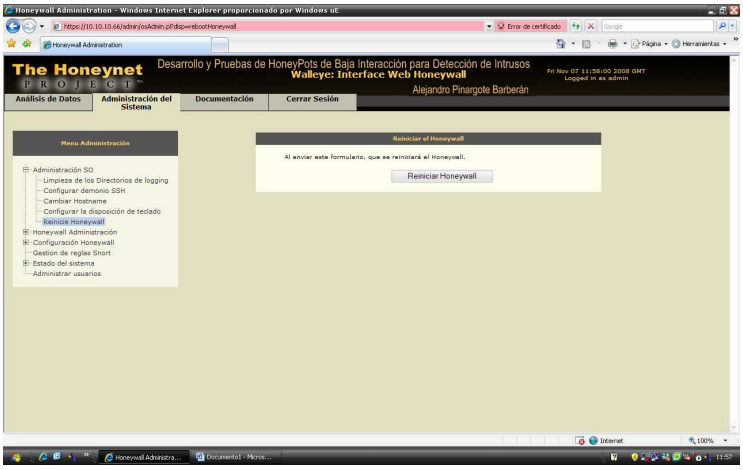
Interfaz de configuración del Hostname del sistema del Honeywall en este caso el Hostname se llama honeywall-espe.



FiguraB. 6: Cambiar Hostname

7. REINICIAR HONEYWALL

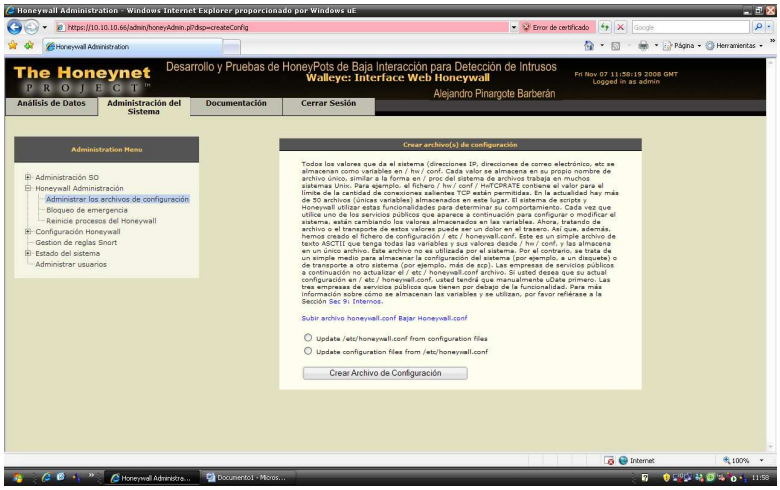
Interfaz donde se encuentra la opción para reiniciar el sistema del Honeywall sin la necesidad de entrar a la configuración del roo.



FiguraB. 7: Reiniciar Honeywall

8. HONEYWALL ADMINISTRACIÓN

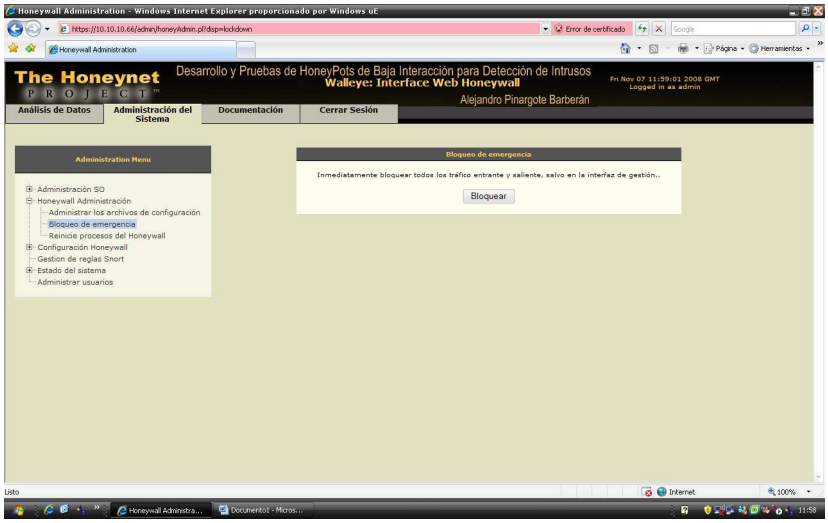
Interfaz que permite la creación de los archivos de configuración del sistema ya sean direcciones ip o direcciones de correo electrónico, al mismo tiempo se puede modificar las conexiones salientes tcp que están permitidas.



FiguraB. 8: Administración Honeywall

9. BLOQUEO DE EMERGENCIA

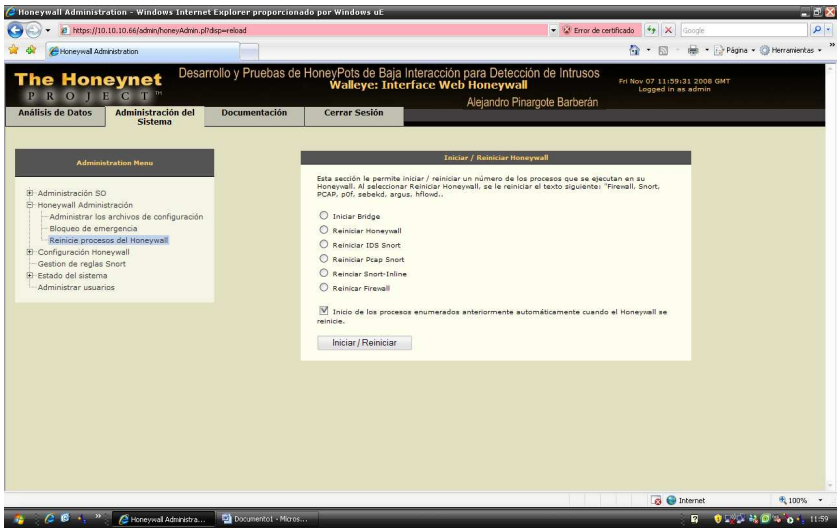
Esta opción permite el bloqueo inmediato de todo el tráfico entrante y saliente menos en la interfaz de gestión.



FiguraB. 9: Bloqueo de Emergencia

10. REINICIO DE LOS PROCESOS HONEYWALL

Interfaz que permite iniciar o reiniciar los diferentes procesos que se encuentran ejecutando en el Honeywall.

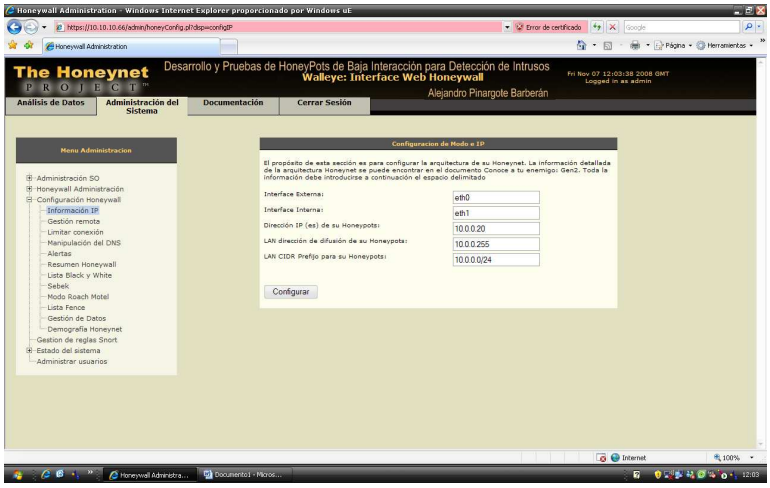


FiguraB. 10: Reinicio de Procesos Honeywall

CONFIGURAR HONEYWALL

11. INFORMACIÓN IP

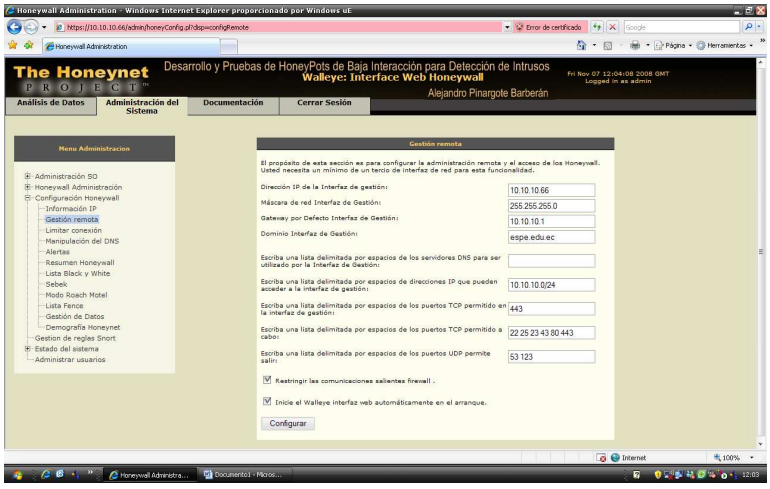
Interfaz que permite la configuración de la arquitectura de la Honeynet ya sean las interfaces internas o externas o las direcciones ip de los Honeypots.



FiguraB. 11: Información IP

12. GESTIÓN REMOTA

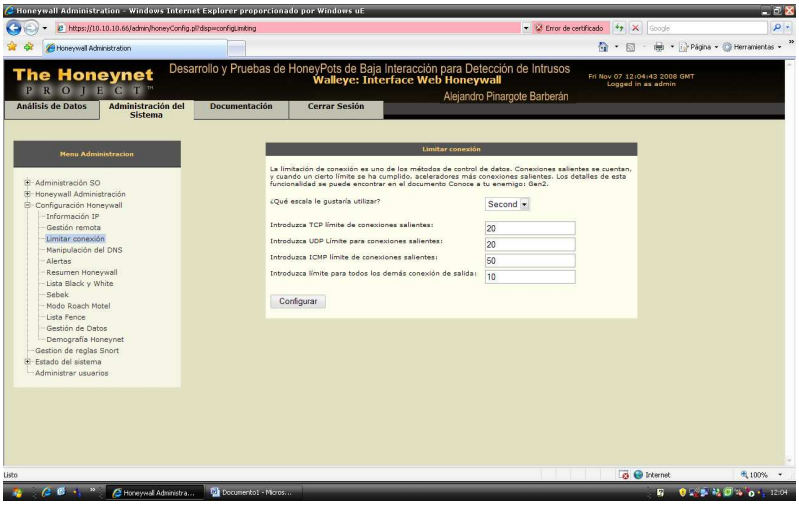
Despliegue de la administración remota y el acceso de los Honeywall. Aquí se configuran los servicios que se van a implementar en el proyecto.



FiguraB. 12: Gestión Remota

13. LIMITAR CONEXIONES

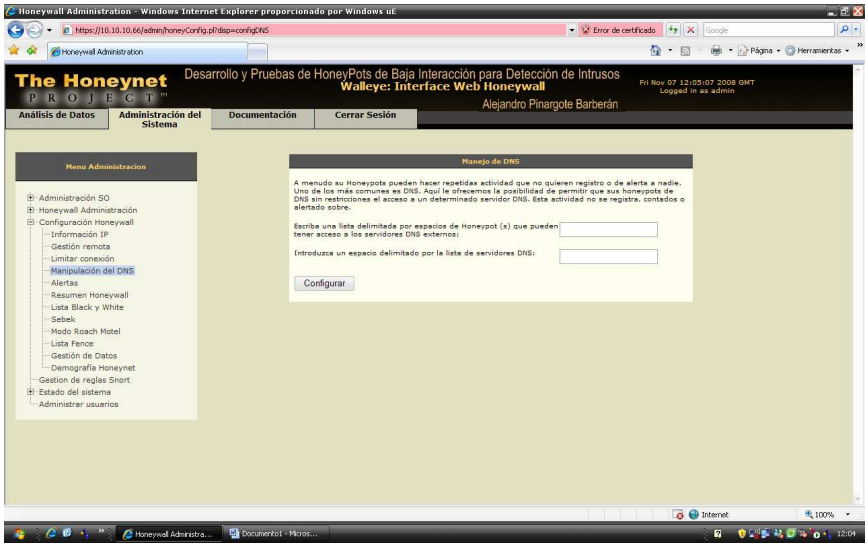
Interfaz en la cual se configura el limite de conexiones salientes ya sean estas TCP, UDP o ICMP.



FiguraB. 13: Limitar Conexiones

14. MANIPULACIÓN DEL DNS

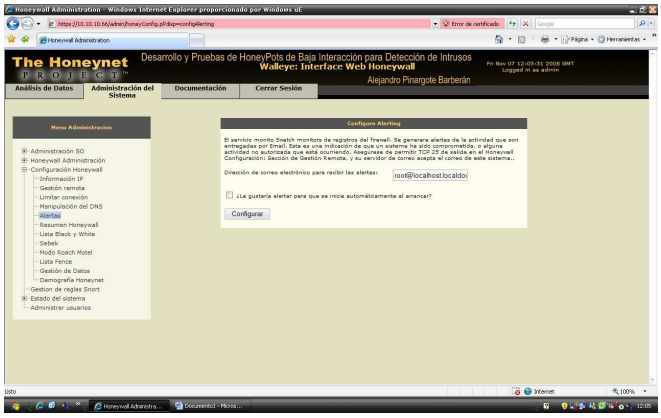
Esta opción permite la posibilidad de que los honeypots tengan acceso a un determinado servidor de DNS sin restricción.



FiguraB. 14: Manipulación del DNS

15. ALERTAS

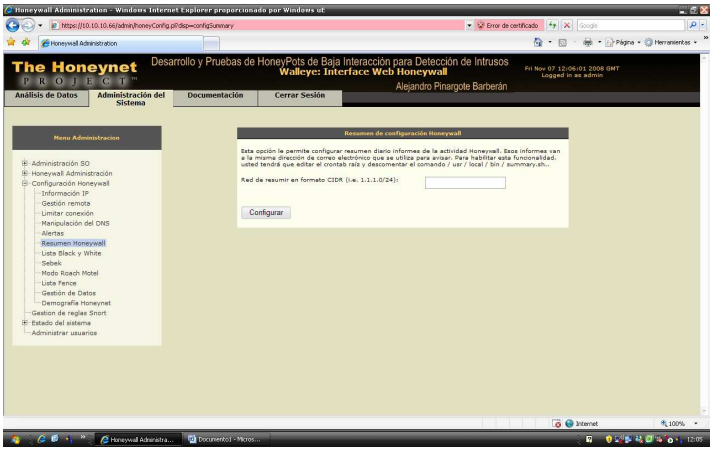
Permite generar alertas para que sean entregadas mediante Email, las cuales pueden ser una actividad no autorizada o algún sistema que se encuentre comprometido.



FiguraB. 15: Alertas

16. RESUMEN DE CONFIGURACIÓN DEL HONEYWALL

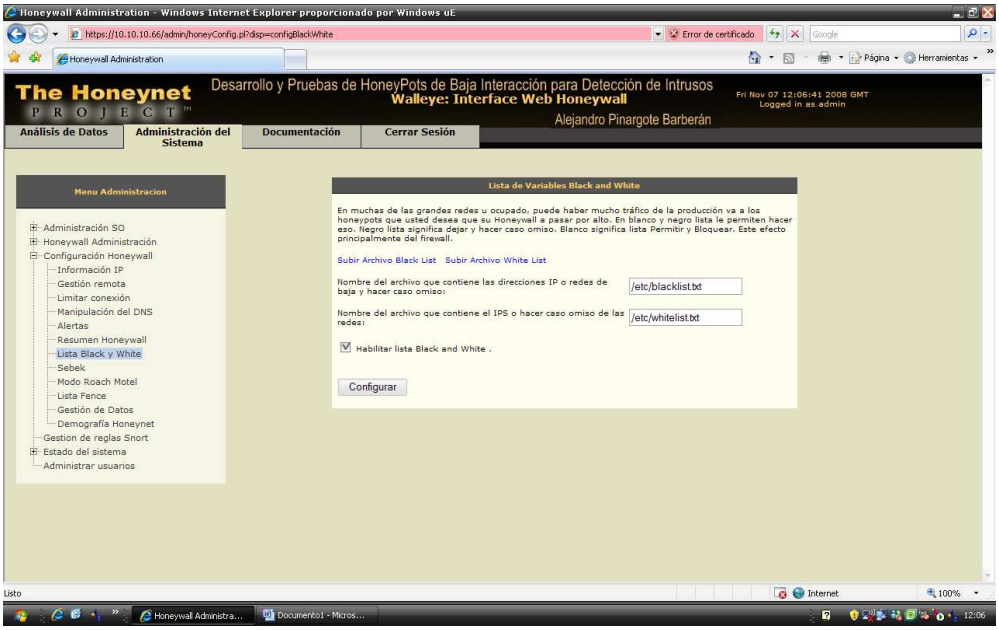
Permite configurar el resumen diario de las actividades realizadas por el Honeywall, los informes serán entregados vía Email a la dirección configurada en la sección anterior



FiguraB. 16: Resumen de Configuración del Honeywall

17. LISTA DE VARIABLES BLACK & WHITE

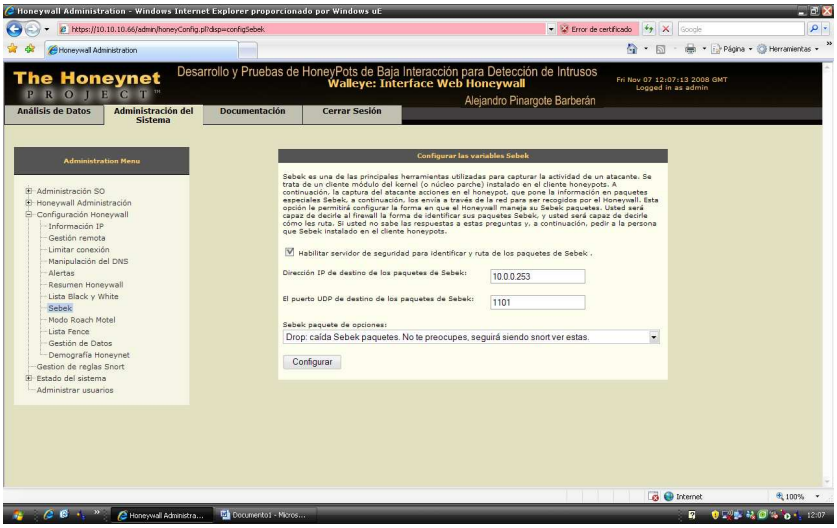
Lista negra es una lista donde se registran las direcciones IPs que generan spam de forma voluntaria o involuntaria, Mientras que una lista blanca, es donde se detalla las direcciones IPs fijadas por el usuario que nunca y bajo ningún concepto los mensajes provenientes de éstas deben ser detectadas y consideradas por el sistema como Spam.



FiguraB. 17: Lista de Variables Black & White

18. CONFIGURACIÓN DE VARIABLES SEBEK

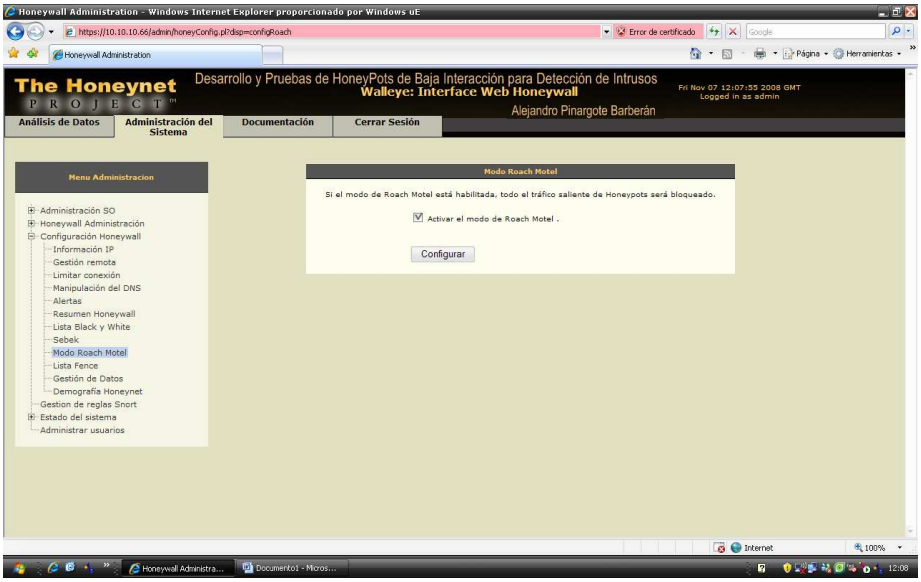
Aquí se configura las variables del sebek para la captura de las actividades del atacante a la vez las envía mediante la red para que sean almacenados en el Honeywall.



FiguraB. 18: Configuración de Variables SEBEK

19. CONFIGURACIÓN DEL MODO ROACH MOTEL

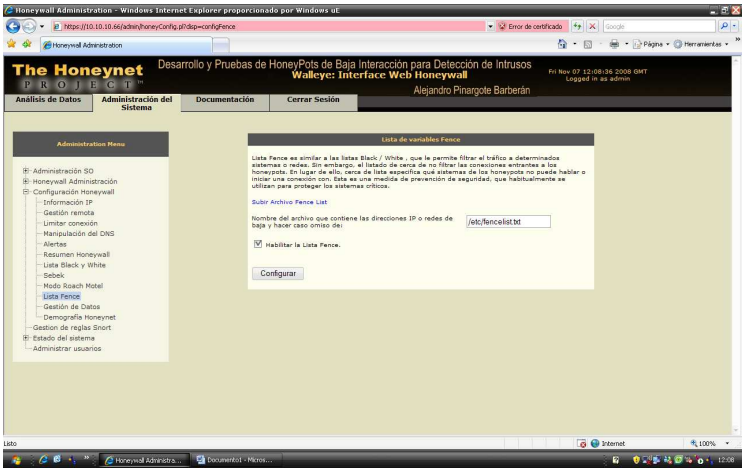
Interfaz que permite bloquear todo el tráfico saliente de los honeypots. Si se habilita Roach motel mode, un atacante podría fácilmente detectar su Honeywall y posteriormente atacarlo, es aconsejable desactivar el bloqueo de todo el tráfico saliente de honeypots.



FiguraB. 19: Configuración del Modo Roach Motel

20. CONFIGURACIÓN DE LAS VARIABLES DE LA LISTA FENCE

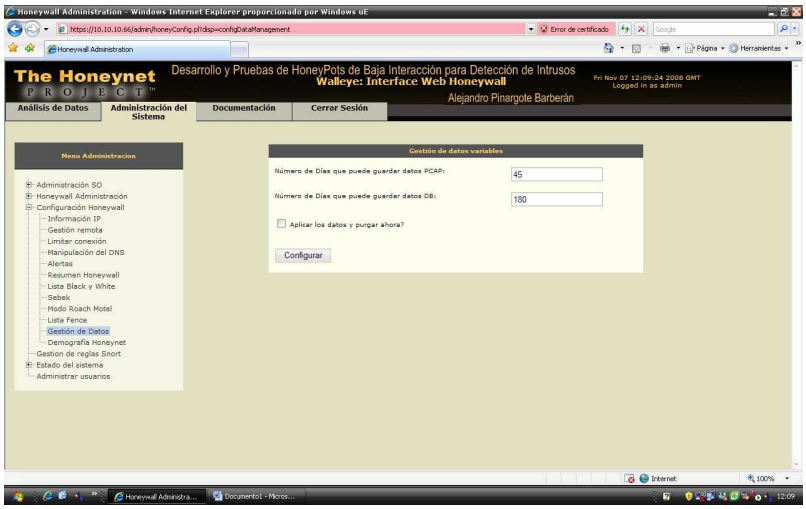
Interfaz que permite a configuración del Fencelist, herramienta que sirve para asegurar las redes de producción. Su aplicación crea reglas en el firewall que bloquee todo el tráfico a determinados objetivos.



FiguraB. 20: Configuración de las Variables de la lista FENCE

21. GESTIÓN DE DATOS VARIABLES

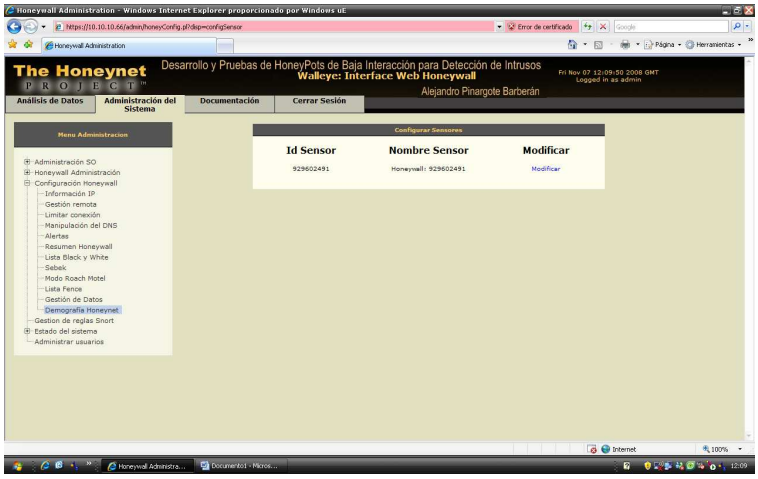
Permite configurar el número de días que quiere que estén almacenados los datos en el PCAP y en la BD.



FiguraB. 21: Gestión de Datos Variables

22. CONFIGURACIÓN DE SENSORES DEL HONEYNET

Permite modificar los sensores del Honeywall ya sean estos el Nombre del Sensor o el Id del Sensor.

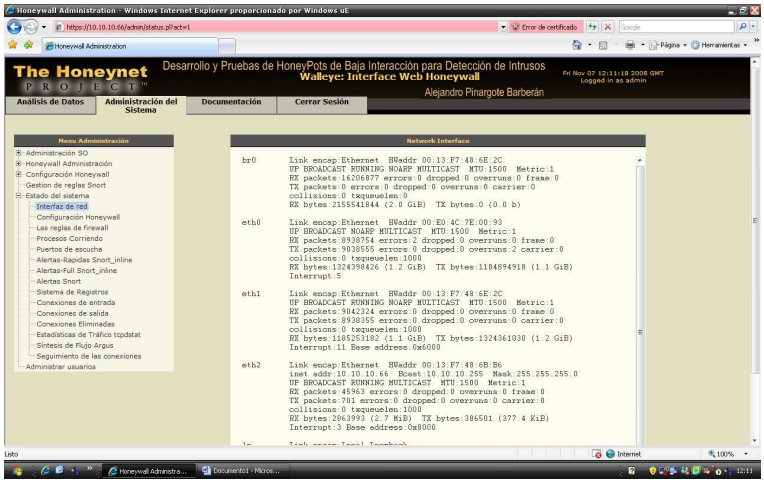


FiguraB. 22: Configuración de Sensores del Honeynet

ESTADO DEL SISTEMA

23. INTERFAZ DE RED

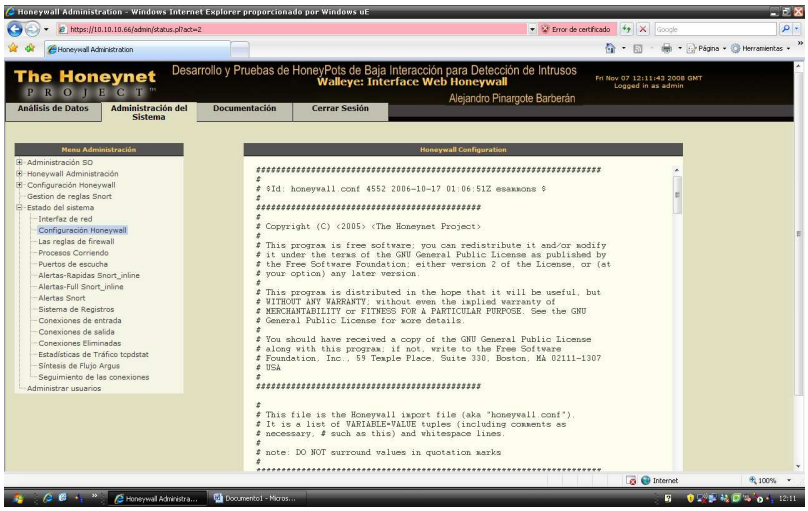
Despliegue de la configuración de las tarjetas de red con las respectivas direcciones IP



FiguraB. 23: Interfaz de Red

24. CONFIGURACIÓN DEL HONEYWALL

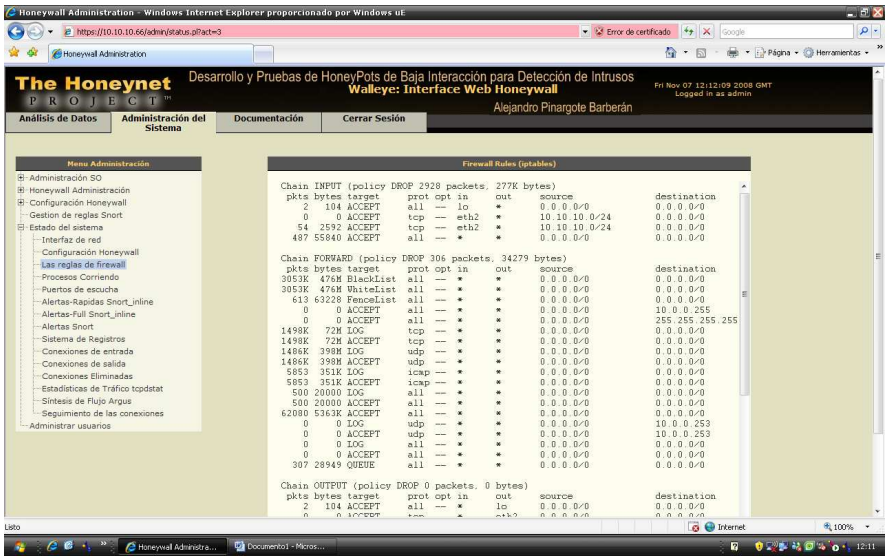
Despliegue del resumen de las configuraciones realizadas en el Honeywall.



FiguraB. 24: Configuración del Honeywall

25. REGLAS DEL FIREWALL

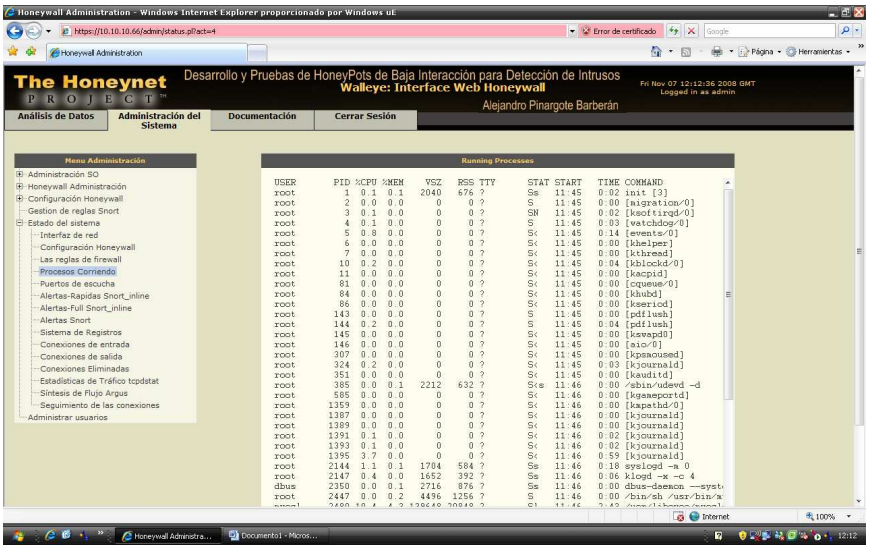
En esta interfaz se despliega las reglas del firewall que tenemos almacenadas en el Honeywall.



FiguraB. 25: Reglas de Firewall

26. PROCESOS EJECUTÁNDOSE

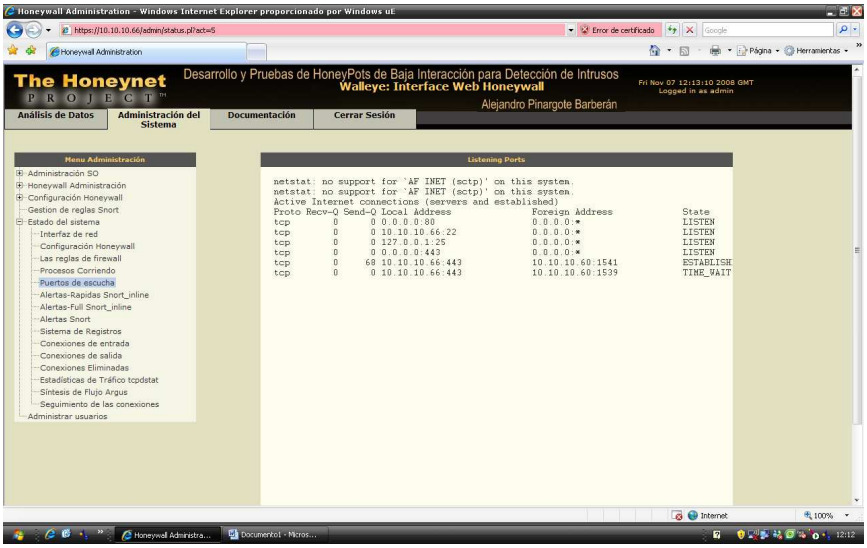
Permite verificar los procesos que se encuentran ejecutándose en el Honeywall.



FiguraB. 26: Procesos Ejecutándose

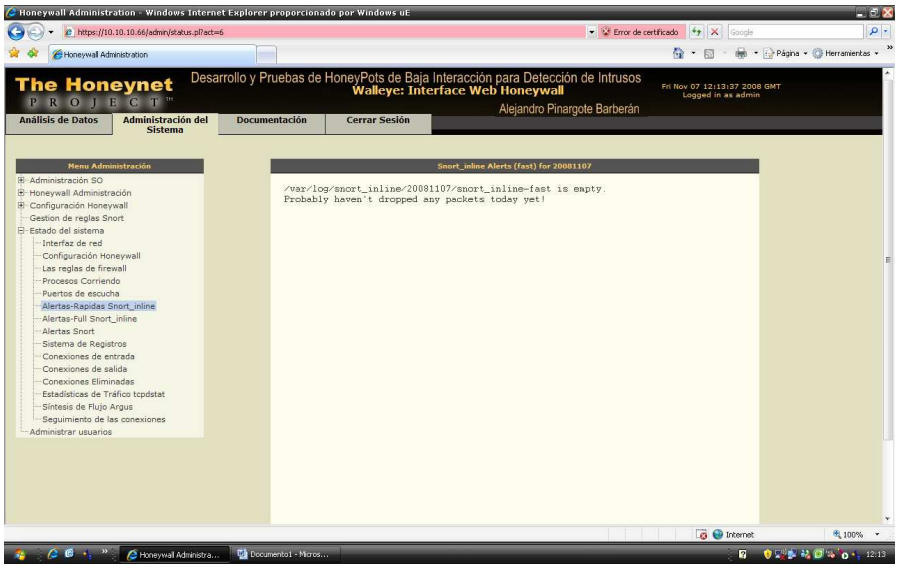
27. PUERTOS DE ESCUCHA

Despliegue de los puertos que se encuentran abiertos en el Honeywall.



FiguraB. 27: Puertos de Escucha

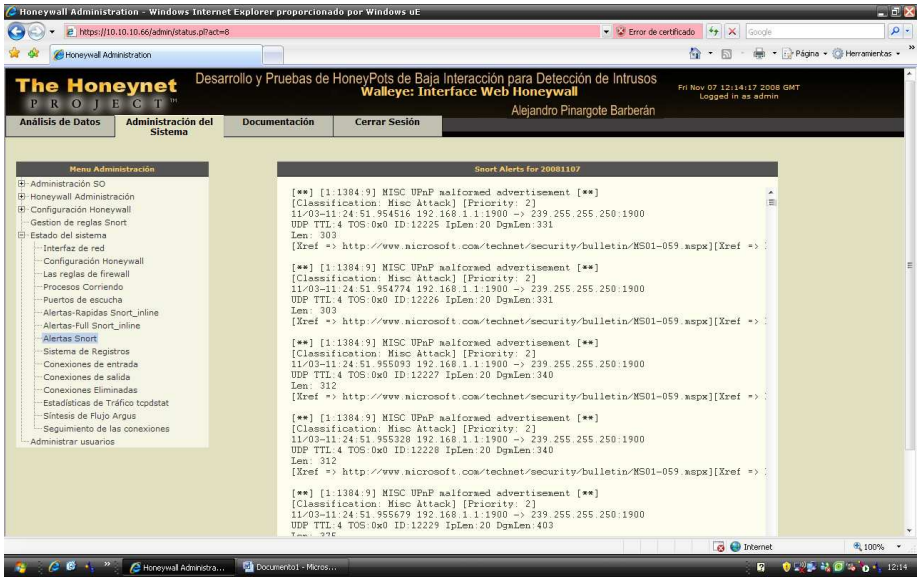
28. ALERTAS RAPIDAS SNORT INLINE



FiguraB. 28: Alertas rápidas Snort Line

29. ALERTAS SNORT

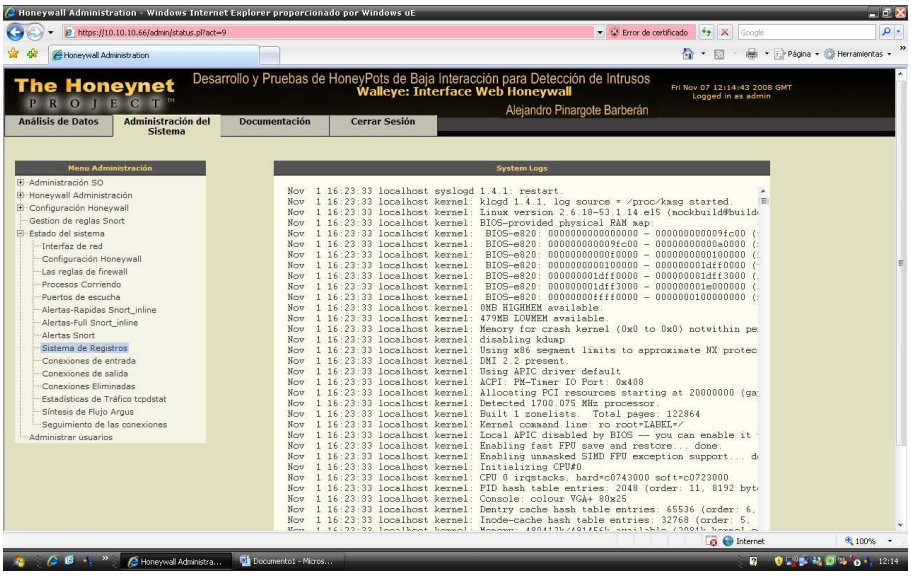
Muestra las alertas detectadas por el Snort de posibles intrusos.



FiguraB. 29: Alertas Snort

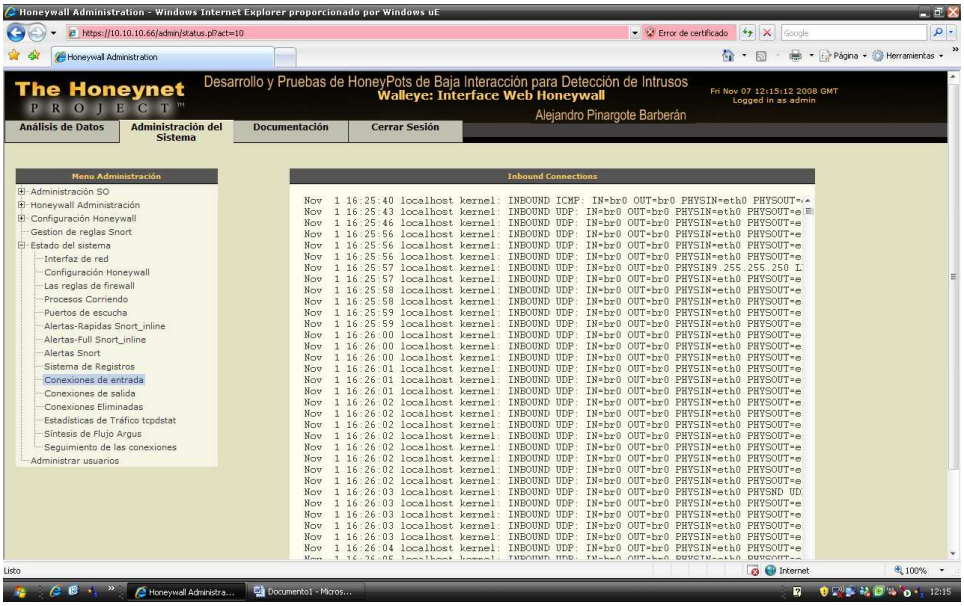
30. SISTEMA DE REGISTRO

Muestra los archivos del sistema configurados.



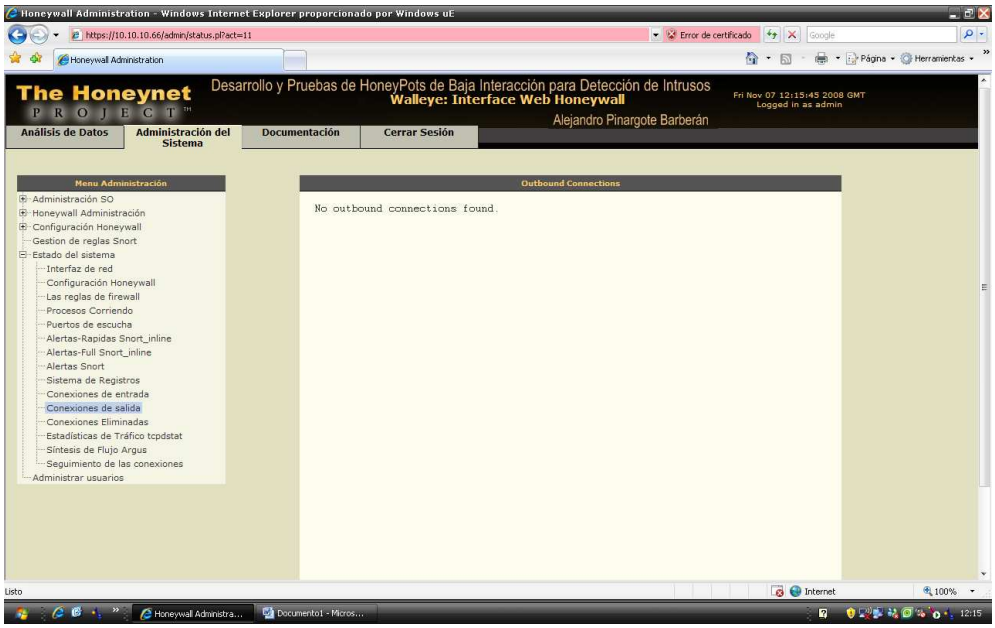
FiguraB. 30: Sistema de Registro

31. CONEXIONES DE ENTRADA



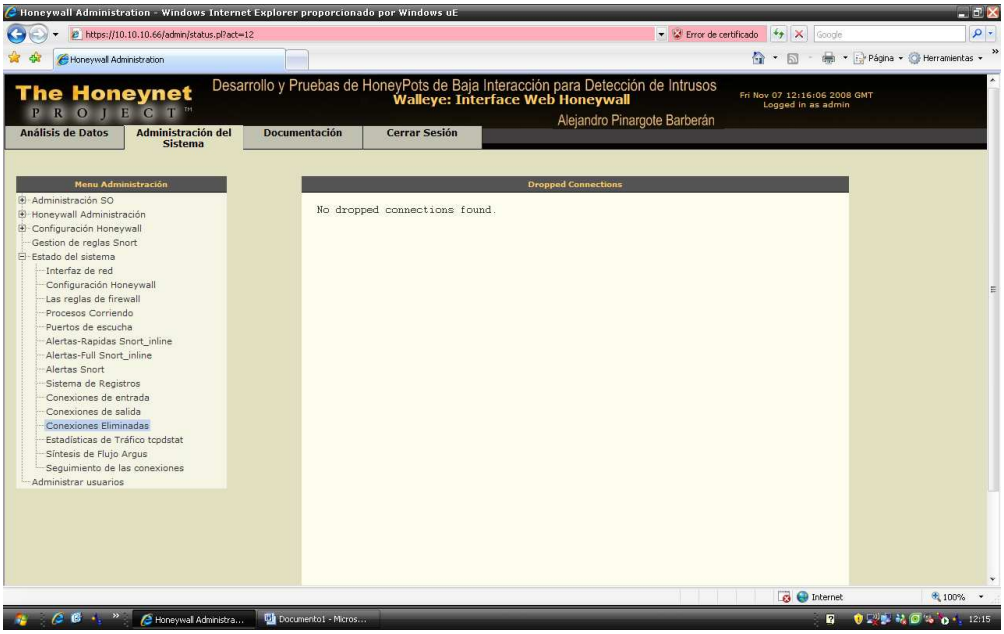
FiguraB. 31: Conexiones de Entrada

32. CONEXIONES DE SALIDA



FiguraB. 32: Conexiones de Salida

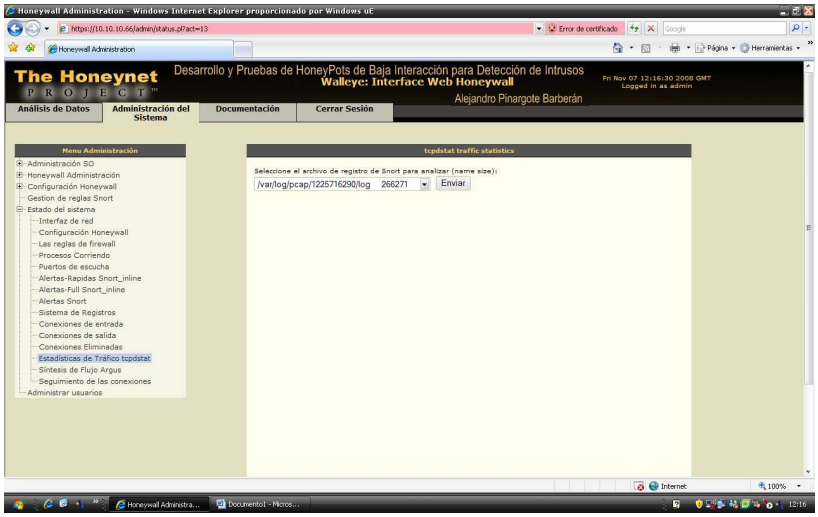
33. CONEXIONES ELIMINADAS



FiguraB. 33: Conexiones Eliminadas

34. ESTADÍSTICAS DE TRÁFICO

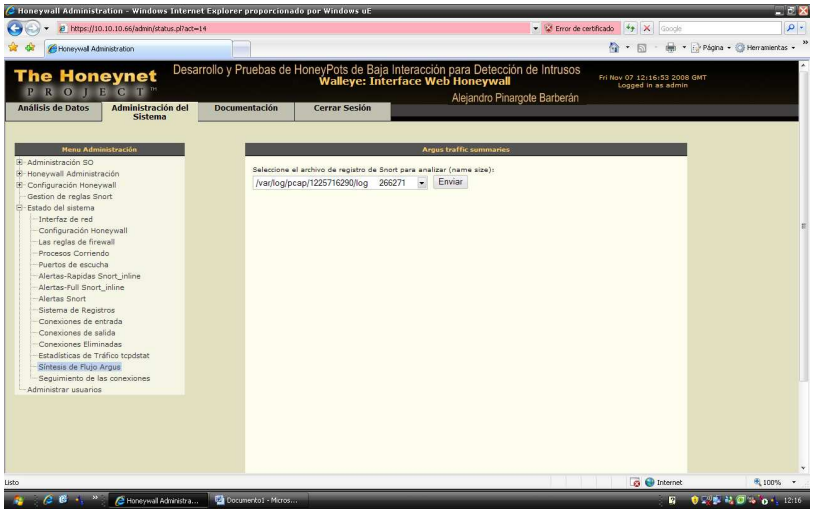
Interfaz en la cual ingresando un archivo del snort genera estadísticas sobre el tráfico generado por un intruso.



FiguraB. 34: Estadísticas de Tráfico

35. SÍNTESIS DE FLUJO ARGUS

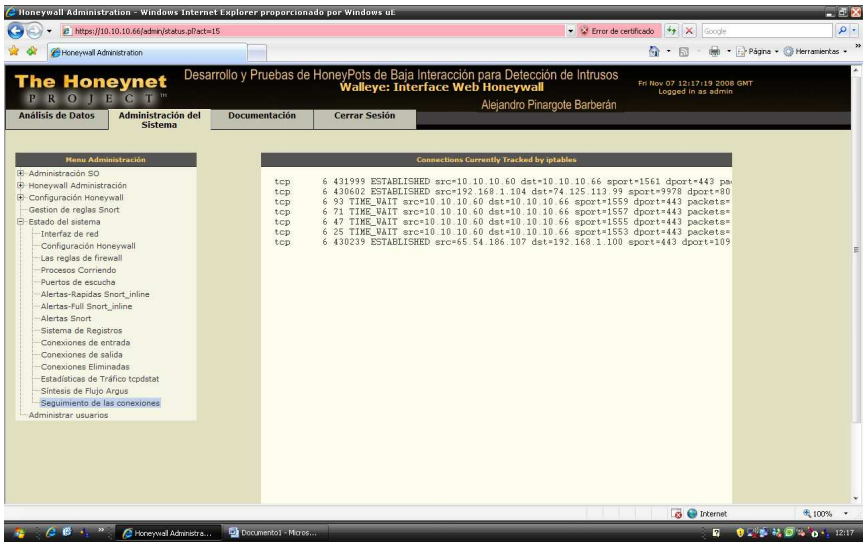
Al igual que en paso anterior permite analizar el trafico generado mediante un registro de Snort.



FiguraB. 35: Síntesis de Flujo Argus

36. SEGUIMIENTO DE LAS CONEXIONES

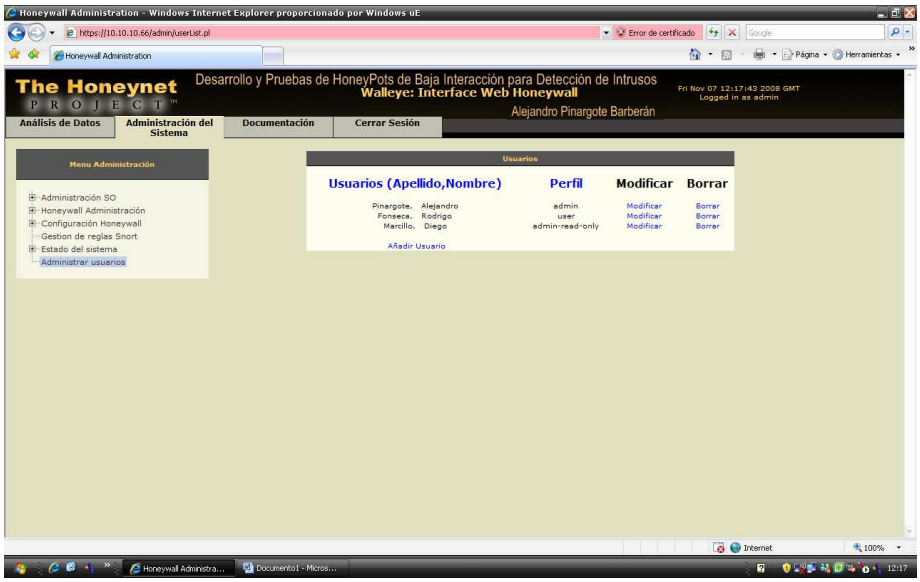
Muestra las conexiones concurrentes por medio de iptables



FiguraB. 36: Seguimiento de las Conexiones

37. ADMINISTRACIÓN DE USUARIOS

Interfaz que muestra los datos de los usuarios con sus respectivas restricciones y permisos para el manejo de la interfaz Web del Honeywall.



FiguraB. 37: Administración de Usuarios

ÍNDICE GENERAL

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS