

## BIBLIOGRAFÍA

### LIBROS

- BACA URBINA, GABRIEL. *Evaluación de Proyectos*. 5<sup>ta</sup> ed. México, MX: McGraw-Hill, 2006. 392 p. ISBN 970-10-5687-6.
- HERNÁNDEZ SAMPIERI, ROBERTO; FERNÁNDEZ-COLLADO, CARLOS; BAPTISTA LUCIO, PILAR. *Metodología de la Investigación*. 4<sup>ta</sup> ed. México, MX: MX: McGraw-Hill, 2006. 850 p. ISBN 970-10-5753-8.
- BONILLA, GILBERTO. *Estadística, Elementos de Estadística Descriptiva y Probabilidad*. 8<sup>va</sup> ed. San Salvador, SV: UCA Editores, 2005. 558 p. ISBN 84-8405-199-4.
- BEJTILICH, RICHARD. *Extrusion Detection: security monitoring for internal intrusions*. 3<sup>ra</sup> ed. California, US: Addison-Wesley Professional, 2005. 416 p. ISBN 978-0321349965.
- DUFF, THOMAS. *Know your Enemy: learning about security threats*. 2<sup>da</sup> ed. California, US: Addison-Wesley Professional, 2004. 800 p. ISBN 978-0321166463.

### INTERNET

- THE HONEYNET PROJECT. *Roo CDROM User's Manual* [en línea]. 1.2 ed. Illinois, US: The Honeynet Project, 2007. [citado 21 de Septiembre de 2006]. Disponible en <<http://www.honeynet.org/tools/cdrom/roo/manual/index.html>>.

- SCOTT, STEVEN. *Snort Installation Manual* [en línea]. 1.5 ed. California, US: Snort Sourcefire Organization, 2002. [citado 17 de Octubre de 2006]. Disponible en <<http://www.snort.org/docs/snort-rh7-mysql-ACID-1-5.pdf>>.
- MATZ, OLIVER. *Official Sebek 2 client for openBSD* [en línea]. 1a. ed. Boston, US: Droids Corporation, 2004. [citado 22 de Octubre de 2006]. Disponible en <<http://honeynet.droids-corp.org/download/sebek-openbsd.pdf>>.
- ANDREASSON, OSKAR. *Iptables Tutorial 1.2.2* [en línea]. 1.1 ed. Boston, US: Free Software Foundation Inc, 2001. [citado 28 de Octubre de 2006]. Disponible en <<http://iptables-tutorial.frozentux.net/iptables-tutorial.html>>.
- GONZALEZ, CESAR. *SNORT+MYSQL+ACID: Sistema de detección de intrusos open source* [en línea]. 2a. ed. Cantabria, ES: LINUCA - Asociación de Usuarios GNU/Linux, 2002. [citado 30 de Octubre de 2006]. Disponible en <<http://www.linuca.org/body.phtml?nIdNoticia=13>>.

## GLOSARIO DE TERMINOS

**Acceso:** Un sujeto o capacidad del objeto para usar, manipular, modificar, o afectar a otro sujeto o el objeto es referido como un acceso. Usuarios autorizados tienen acceso legal a un sistema, mientras que los hacker tienen acceso ilegal al sistema.

**Activo:** Es un recurso de la organización que está siendo protegido. Un activo podría ser lógico como los datos o físico como una persona o un computador personal.

**Ataque:** Es un acto que es intencional que busca hacer daño o comprometer la información y/o los sistemas que soporta.

**Ataque activo:** Acción deliberada de un atacante para obtener acceso a la información y los atacantes están activamente haciendo intentos para penetrar en la organización.

**Ataque pasivo:** Está orientado en recopilar la información en comparación con el acceso a ella directamente para luego lanzar un ataque activo.

**Cracker:** Es un hacker que irrumpe en sistemas informáticos ajenos para aprovecharse de otros, robar o, sencillamente, crear problemas.

**DTC:** Dirección de tecnología y comunicaciones, departamento en la universidad Francisco Gavidia encargado de las comunicaciones del campus.

**DoS:** un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Se genera mediante la saturación de

los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no de abasto a la cantidad de usuarios.

**Enrutador:** Un router, en español enrutador, ruteador o encaminador es un dispositivo de hardware para interconexión de redes de ordenadores que opera en la capa tres (nivel de red). Un router es un dispositivo que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

**Firewall:** Un cortafuegos (o firewall en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

**Hacker:** Procede del inglés "hack" (recortar) y es la palabra utilizada en determinados ámbitos de las nuevas tecnologías para denominar las pequeñas modificaciones que se le pueden hacer a un programa.

**Honeynet:** Son un tipo especial de Honeypots de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes. Se usan equipos reales con sistemas operativos reales y corriendo aplicaciones reales.

**Honeypot:** Es un software o conjunto de computadores cuya intención es atraer a crackers, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Los Honeypots pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque al honeypot.

**IDS:** Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos desautorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers que usan herramientas automáticas.

**Información:** Los datos se perciben mediante los sentidos, éstos los integran y generan la información necesaria para producir el conocimiento que es el que finalmente permite tomar decisiones para realizar las acciones cotidianas que aseguran la existencia social

**Intrusión (Exploit):** Hay dos formas comunes de esta palabra en términos de seguridad, primero los hacker pueden atentar a una intrusión a un sistema de información usándolo ilegalmente. Segundo una intrusión puede ser un blanco de una solución para un uso inadecuado por una vulnerabilidad para formular un ataque.

**Iptables:** Es una herramientas de cortafuegos que permite filtrar paquetes, realizar traducción de direcciones de red (NAT) para IPv4 y mantener registros de log.

**Kernel:** En informática, el núcleo (también conocido en español con el anglicismo kernel, de raíces germánicas como kern) es la parte fundamental de un sistema operativo. Es el software responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma más básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.

**Linux:** Es la denominación de un sistema operativo tipo Unix (también conocido como GNU/Linux) y el nombre de un núcleo. Es uno de los ejemplos más prominentes del software libre y del desarrollo del código abierto, cuyo código fuente está disponible públicamente, para que cualquier persona pueda libremente usarlo, estudiarlo, redistribuirlo, comercializarlo y, con los conocimientos informáticos adecuados, modificarlo.

**Malware:** Del inglés malicious software, también (del inglés llamado badware o software malicioso) es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría.

**Red Hat:** Es la compañía responsable de la creación y mantenimiento de una distribución del sistema operativo GNU/Linux que lleva el mismo nombre: Red Hat Enterprise Linux, y de otra más, Fedora.

**Script:** En informática, un script es un guión o conjunto de instrucciones. Permiten la automatización de tareas creando pequeñas utilidades. Es muy utilizado para la administración de sistemas UNIX. Son ejecutados por un intérprete de línea de órdenes y usualmente son archivos de texto. También Script Puede considerarse una alteración o acción a una determinada plataforma.

**Sebek:** Es un módulo de Kernel que captura las teclas pulsadas por el intruso y los ficheros descargados por este en el sistema comprometido. Este software se oculta en el sistema para evitar ser detectado o desinstalado y envía la información recopilada al servidor remoto.

**Sniffer:** En informática, es un programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad de investigación, aunque también puede ser utilizado con fines maliciosos.

**Snort:** Es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL. Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.

**Sistema:** Cualquier conjunto cohesionado de elementos que están dinámicamente relacionados para lograr un propósito determinado.

**Sistema de Información (SI):** Parte de un sistema general de información que emplea el equipo, los métodos y los procedimientos necesarios para procesar la información por medios electrónicos.

**Troyano:** Se denomina troyano (o caballo de Troya, traducción fiel del inglés Trojan horse aunque no tan utilizada) a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona.

**Virus:** Es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Aunque popularmente se incluye al "malware" dentro de los virus, en el sentido estricto de esta ciencia los virus son programas que se replican y ejecutan por sí mismos. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos.

**VMWare:** Es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (un ordenador, un hardware) con unas características hardware determinadas. Cuando se ejecuta el programa (simulador), proporciona un ambiente de ejecución similar a todos los efectos a un ordenador físico (excepto en el puro acceso físico al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB y disco duro.

**Vulnerabilidad:** En términos de Seguridad de la Información, una vulnerabilidad es una debilidad en los procedimientos de seguridad, diseño, implementación o control interno que podría ser explotada (accidental o intencionalmente) y que resulta en una brecha de seguridad o una violación de la política de seguridad de sistemas.

## **ANEXO A**

### **Instalación y configuración básica del sistema operativo Red Hat 9.0**

En su gran mayoría, todos los sistemas operativos utilizan particiones de discos, y Red Hat Linux no es una excepción. Cuando se instale Red Hat Linux, se tendrá de realizar particiones de disco. Si Red Hat Linux va a compartir el sistema con otro sistema operativo se necesitará estar seguro de tener espacio disponible suficiente en lo(s) disco(s) duro(s) para la instalación. El espacio de disco destinado a Red Hat Linux debe estar separado del espacio utilizado por otros sistemas operativos que puedan estar instalados en su sistema, como por ejemplo Windows, OS/2, o incluso una versión diferente de Linux.

Antes de comenzar el proceso de instalación, deberán reunirse al menos una de las condiciones siguientes:

- La computadora deberá tener espacio sin particionar para la instalación de Red Hat Linux.
- Deberá contar con una o más particiones que pueda borrar para conseguir más espacio libre para instalar Red Hat Linux.

#### **Instalación de tipo - Estación de trabajo**

Una instalación de tipo estación de trabajo, incluye un entorno de escritorio gráfico y herramientas de desarrollo de software, requiere al menos 2.1 GB de espacio libre. Si escoge los dos entornos de escritorio GNOME y KDE necesitará al menos 2.2 GB de espacio libre.



## **Instalación de tipo - Servidor**

Una instalación de tipo servidor requiere 850 MB en una instalación mínima sin X (el entorno gráfico en el sistema operativo), al menos 1.5 GB de espacio libre en disco si todos los componentes que no sean X (grupos de paquetes) están instalados y, al menos, 5.0 GB para instalar todos los paquetes incluidos los entornos GNOME y KDE.

## **Instalación de tipo - Escritorio personal**

Una instalación de tipo escritorio personal, habiendo elegido instalar GNOME o KDE, requiere al menos 1.7GB de espacio libre. Si selecciona ambos entornos de escritorio, necesitará al menos 1.8GB de espacio libre en disco. En este caso en particular se realizará la instalación del tipo de escritorio personal para la mayoría de los computadores en la honeynet.

## **Instalación desde un CD-ROM**

Para instalar Red Hat Linux desde un CD-ROM, escoja CD-ROM y seleccione OK. Cuando el programa se lo indique, inserte el CD de Red Hat Linux en el lector de disco (si no arrancó desde una unidad de CD). Una vez que el CD esté en la unidad de CD-ROM, seleccione OK, y presione Intro.

El programa de instalación probará su sistema e intentará identificar su lector de CD-ROM. En primer lugar, buscará un lector de CD-ROM IDE (también conocido como ATAPI)

## **Bienvenida a Red Hat Linux**

La pantalla de bienvenida no le pedirá ninguna información. Por favor lea el texto de ayuda en el panel de la izquierda para instrucciones adicionales e información sobre el registro de su producto Red Hat Linux.

Observe que el botón “Esconder ayuda” se encuentra en la parte inferior izquierda de la pantalla. La pantalla de ayuda aparece abierta por defecto. Si no quiere visualizar la información, haga clic en “Esconder ayuda” para minimizar esta parte de la pantalla. Haga clic en “siguiente” para continuar.

## Selección del idioma

Utilizando su ratón, elija el idioma que quiere usar por defecto para la instalación y para el sistema, ver la figura 13. El programa de instalación intentará definir el huso horario adecuado basándose en su configuración.



Figura 13. Selección de idioma.

Una vez que haya seleccionado el idioma, haga clic en “siguiente” para continuar.

## Configuración del teclado

Con el ratón, elija el tipo de teclado que mejor se adapte a su sistema, ver la figura 14. Haga clic en “Siguiente” para continuar.



Figura 14. Selección de teclado.

Para cambiar la disposición del teclado después de haber completado la instalación, use la herramienta de configuración de teclados. Escriba el comando redhat-config-keyboard en una línea de comandos del shell para lanzar la Herramienta de configuración de teclados. Si no es root, se le pedirá que se introduzca la contraseña de root para continuar.

## Configuración del ratón

Elija el ratón adecuado a su sistema. Si no encuentra el tipo exacto, elija el que crea que será compatible con el suyo. Para determinar la interfaz del ratón, observar el conector de su ratón y siga los siguientes diagramas. Si está

instalando Red Hat Linux en una computadora portátil, en la mayoría de los casos el dispositivo en cuestión será compatible con PS/2.

Si no encuentra un ratón del que esté seguro que es compatible con su sistema, seleccione una de las entradas Generic, basadas en el número de botones de su ratón y de su interfaz. Si tiene un ratón de scroll, seleccione la entrada Generic - Wheel Mouse (con el puerto del ratón correcto) como un tipo de ratón compatible.

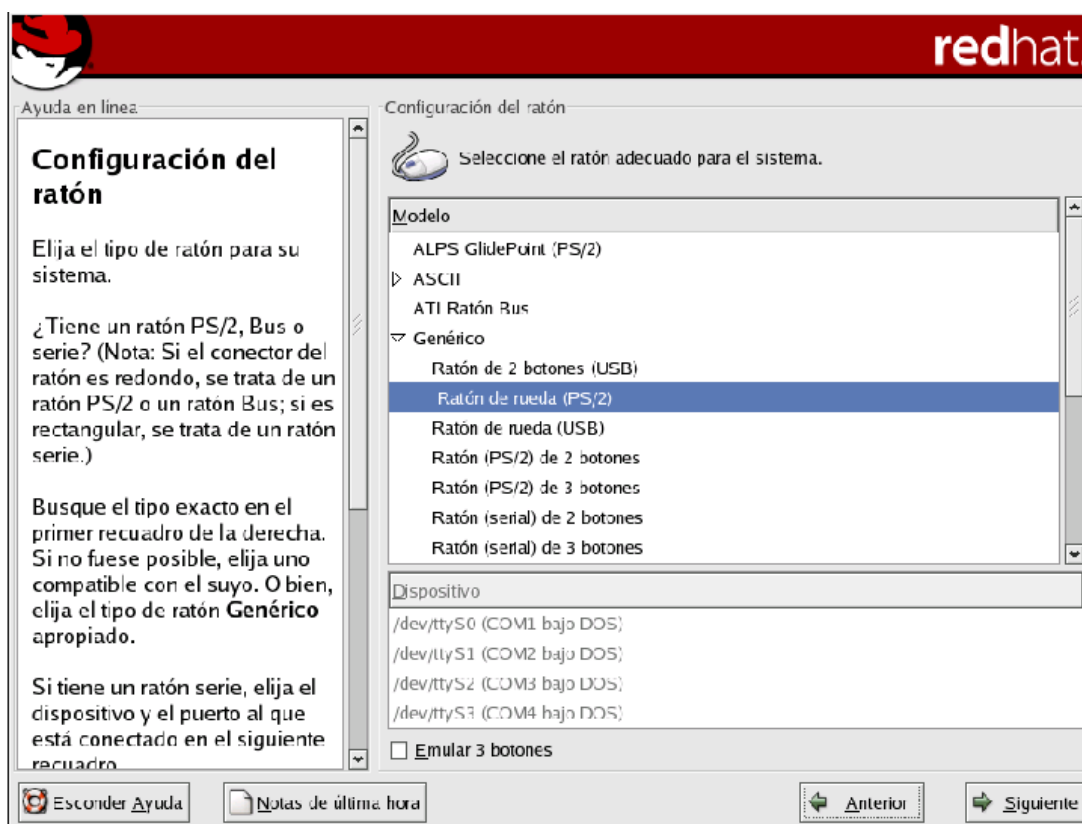


Figura 15. Selección del ratón

## Seleccionar actualizar o instalar

La pantalla “Examinar la actualización” aparece automáticamente si el programa de instalación detecta una versión previa de Red Hat Linux en su sistema. Si desea llevar a cabo una actualización, seleccione Actualizar una instalación existente. Asegúrese de seleccionar personalizar los paquetes a actualizar si desea tener mayor control sobre cuáles paquetes serán actualizados en su

sistema. Para realizar una nueva instalación de Red Hat Linux en su sistema, seleccione Realizar una nueva instalación de Red Hat Linux y haga clic en Siguiente.

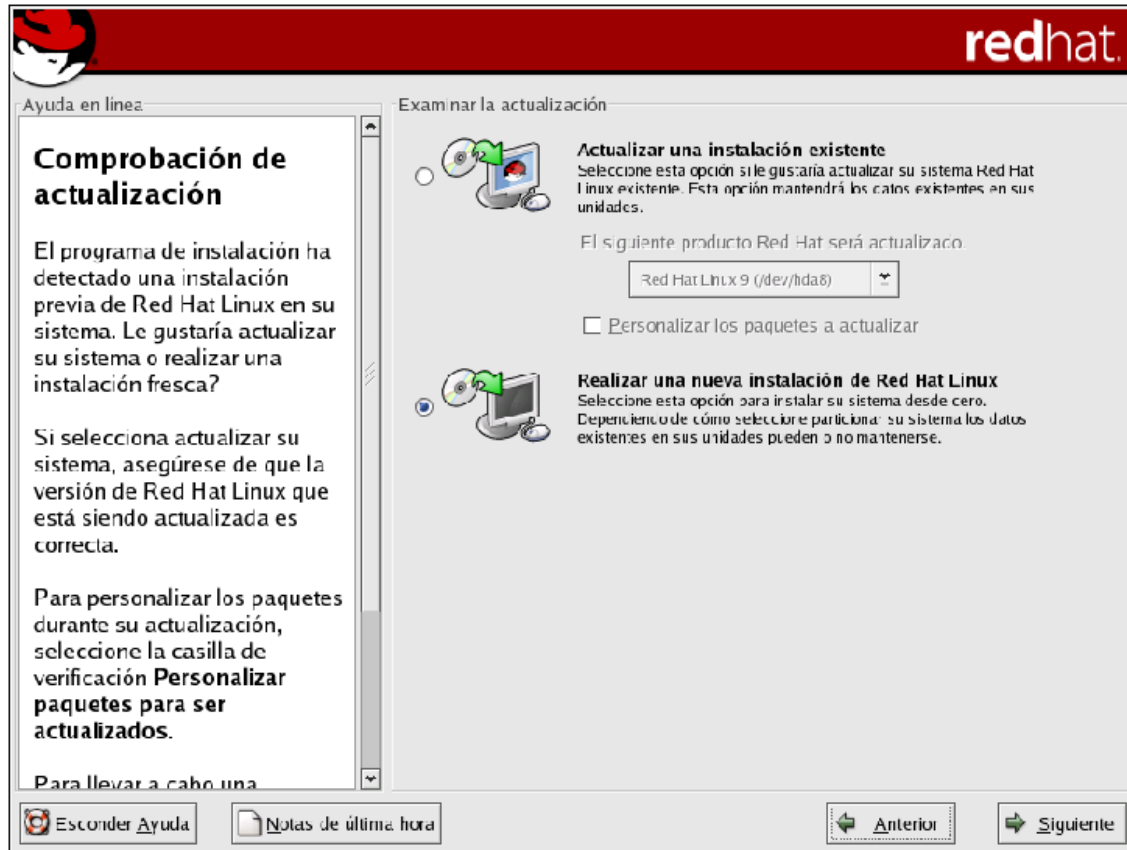


Figura 16. Selección de instalación de Red Hat

## Opciones de instalación

Elija qué tipo de instalación desea realizar. El sistema Red Hat Linux le permitirá elegir el tipo de instalación que mejor se ajuste a sus necesidades. Las opciones disponibles son: Estación de trabajo, Servidor, Portátil, Personalizada y Actualización.



Figura 17. Selección de tipo de instalación.

## Configuración del particionamiento del disco

El particionamiento le permite dividir el disco duro en secciones aisladas, donde cada sección se comporta como su propio disco duro. El particionamiento es especialmente útil si ejecuta más de un sistema operativo. En esta pantalla, puede elegir entre realizar un particionamiento automático o un particionamiento manual con Disk Druid. El particionamiento automático le permite realizar una instalación sin tener que particionar los discos. En este caso se elegirá la partición automática, a fin de que el proceso de instalación qué tipo de partición adoptar. Para particionar de forma manual, escoja la herramienta de particionamiento Disk Druid.

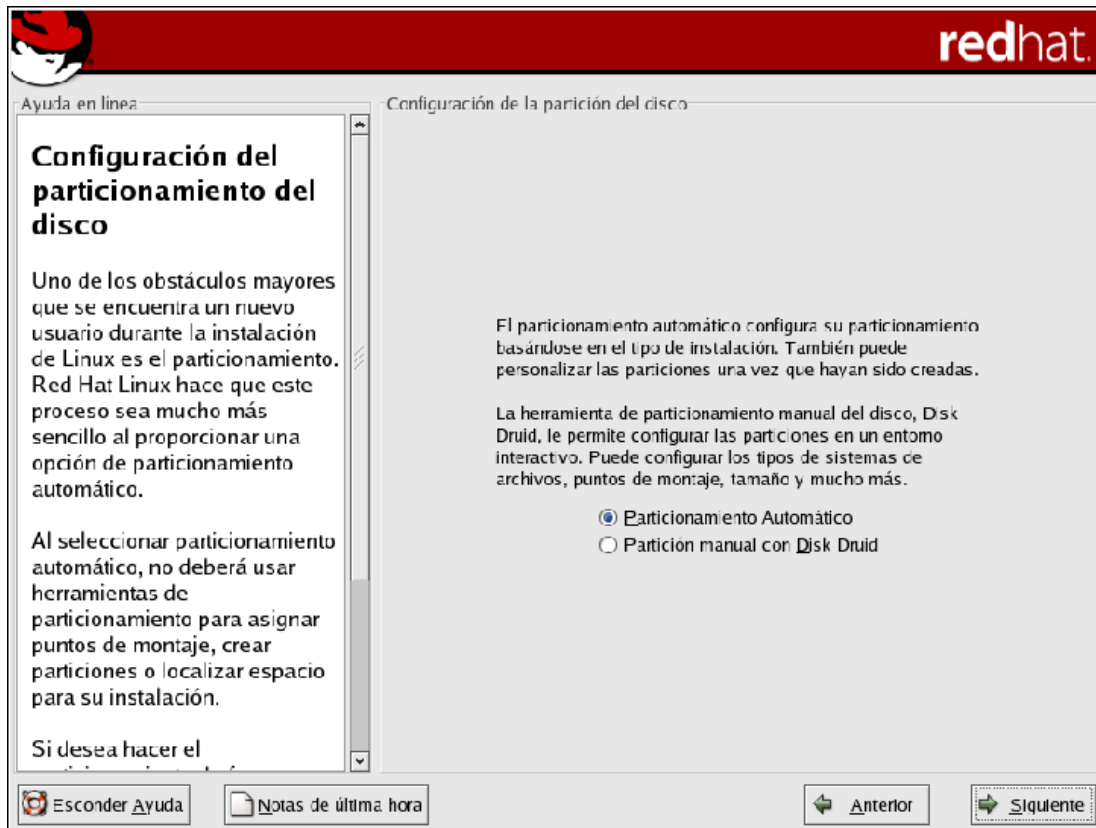


Figura 18. Selección de tipo de partición.

## Particionamiento automático

El particionamiento automático le permite tener control de los datos que se han eliminado en su sistema. Tiene las siguientes opciones:

- Eliminar todas las particiones Linux del sistema: seleccione esta opción para eliminar tan sólo las particiones Linux (particiones creadas en una instalación Linux previa). No borrará el resto de particiones que tenga en el disco(s) duro(s) (tal como VFAT o particiones FAT32).
- Eliminar todas las particiones del sistema: seleccione esta opción para eliminar todas las particiones de su disco duro (esto incluye las particiones creadas por otros sistemas operativos tales como Windows 95/98/NT/2000).

Si selecciona esta opción, todos los datos en el disco seleccionado serán eliminados por el programa de instalación. No seleccione esta opción si tiene información que desea mantener en los discos duros en los que está instalando Red Hat Linux. Mantener todas las particiones y usar el espacio libre existente: seleccione esta opción para conservar los datos y las particiones actuales, presumiendo que tiene suficiente espacio disponible en los discos duros.

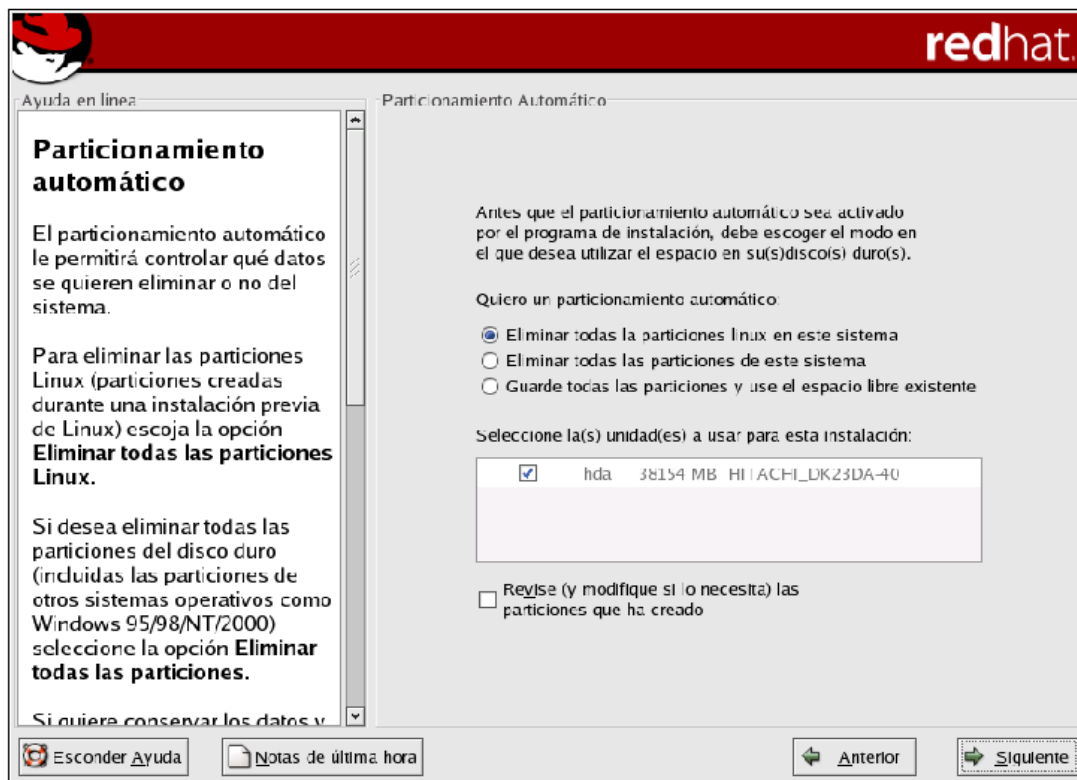


Figura 18. Particionamiento automático.

Mediante el uso del ratón, escoja los discos duros en los que quiere instalar Red Hat Linux. Si tiene dos o más discos duros, puede escoger qué disco duro debería contener esta instalación. Esto no repercutirá a los discos duros no seleccionados ni a ninguno de sus datos.



Para revisar y realizar los cambios necesarios en las particiones creadas con el particionamiento automático, seleccione la opción Revisar. Después de seleccionar Revisar y hacer clic en “siguiente” para continuar, verá las particiones creadas en la aplicación Disk Druid. También podrá modificar estas particiones si no cumplen sus necesidades. Haga clic en “siguiente” una vez que haya hecho sus selecciones para continuar.

## **Campos de la partición**

Las diferentes etiquetas de cada partición presentan información sobre las particiones que está creando. Las etiquetas son las que siguen a continuación:

- **Dispositivo:** Este campo muestra el nombre del dispositivo de la partición.
- **Punto de montaje:** Un punto de montaje es el lugar en la jerarquía de directorios a partir del cual un volumen existe; el volumen se "monta" en este lugar. Este campo indica dónde se montará la partición. Si la partición existe pero no se ha definido un punto de montaje, necesitará definir uno. Haga doble clic sobre la partición o en el botón “modificar” para cambiar los parámetros de la partición.
- **Tipo:** Este campo muestra el tipo de partición (por ejemplo, ext2, ext3, o vfat).
- **Formato:** Este campo muestra si la partición que se está creando se formateará.
- **Tamaño:** Este campo muestra el tamaño de la partición (en MB).
- **Comienzo:** Este campo muestra el cilindro en su disco duro donde la partición comienza.
- **Final:** Este campo muestra el cilindro en su disco duro donde la partición termina.

Ocultar los miembros del grupo del dispositivo RAID/volumen LVM: Seleccione esta opción si no desea visualizar los miembros del grupo del dispositivo RAID o del volumen LVM que se han creado.

## **Esquema de particionamiento recomendado**

Una partición swap (de al menos 32 MB): Las particiones swap se usan para soportar la memoria virtual. En otras palabras, los datos se escriben en la partición swap cuando no hay suficiente RAM para almacenar los datos que su sistema está procesando. El tamaño mínimo de la partición swap debería ser igual al doble de la cantidad de memoria RAM que tiene el sistema o 32 MB.

Por ejemplo, si tiene 1 GB de RAM o menos, su partición swap debería ser al menos igual a la cantidad de RAM de su sistema, hasta dos veces el tamaño de la memoria RAM. Para más de 1 GB de RAM, se recomiendan 2GB de swap. La creación de una partición de espacio swap de gran tamaño será especialmente útil si desea actualizar su RAM en un momento posterior.

Una partición /boot (100MB) — la partición montada sobre /boot contiene el kernel del sistema operativo (que permitirá al sistema arrancar Red Hat Linux), junto a otros archivos utilizados para el proceso de arranque. Debido a las limitaciones de la mayoría de las BIOS de los ordenadores, se aconseja crear una partición pequeña para guardar estos archivos. Para la mayoría de los usuarios, una partición de arranque de 75 MB es suficiente.

## **Configuración de red**

La siguiente pantalla se desplegará para la configuración de la tarjeta de red.

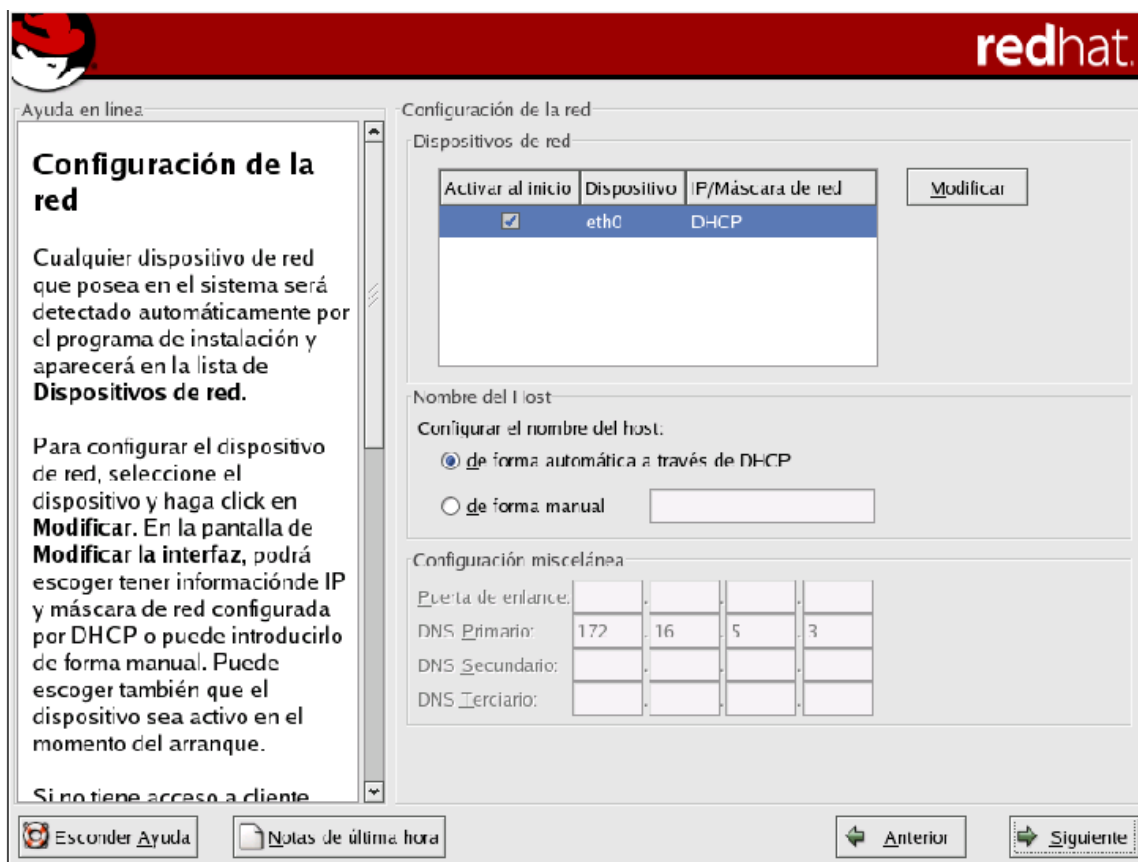


Figura 19. Instalación de tarjeta de red.

El programa de instalación automáticamente detecta los dispositivos de red que tiene y los muestra en la lista Dispositivos de red. Una vez que haya seleccionado el dispositivo de red, haga clic en “modificar”. En la pantalla desplegable modificar interfaz puede elegir la dirección IP o la máscara de red del dispositivo con el DHCP (o manualmente si no ha seleccionado DHCP) y puede también activar el dispositivo en el intervalo de arranque. Si selecciona Activar en arranque, el dispositivo de red arrancará cuando arranque el sistema. Si no tiene el acceso al cliente DHCP.

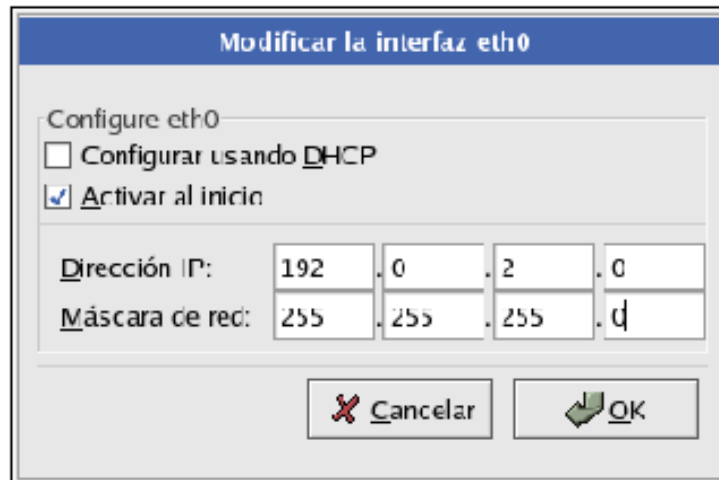


Figura 20. Modificación de parámetros de dirección IP.

## Configuración del cortafuegos

Red Hat Linux también le ofrece protección vía cortafuegos (firewall) para una seguridad mejorada del sistema. Un cortafuegos se dispone entre su ordenador y la red y determina qué recursos de su equipo están accesibles para los usuarios remotos de la red. Un cortafuegos bien configurado puede aumentar significativamente la seguridad de su sistema. En este caso no se realizará ninguna configuración de firewall.

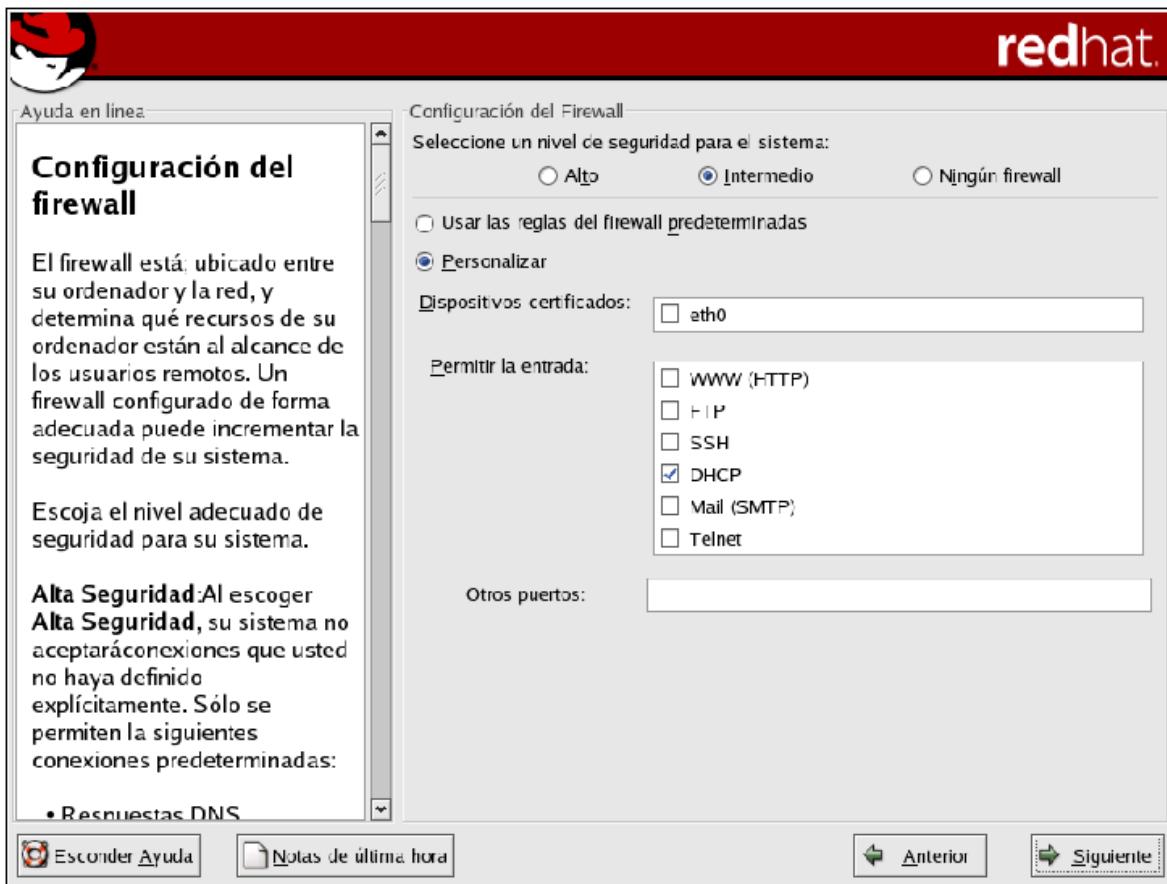


Figura 21. Configuración de cortafuegos.

## Configuración de la contraseña de root

La configuración de la cuenta y la contraseña root es uno de los pasos más importantes durante la instalación. La cuenta root es similar a la cuenta del administrador usada en las máquinas Windows NT. La cuenta root es usada para instalar paquetes, actualizar RPMs y realizar la mayoría de las tareas de mantenimiento del sistema. Conectándose como root le da control completo sobre el sistema.

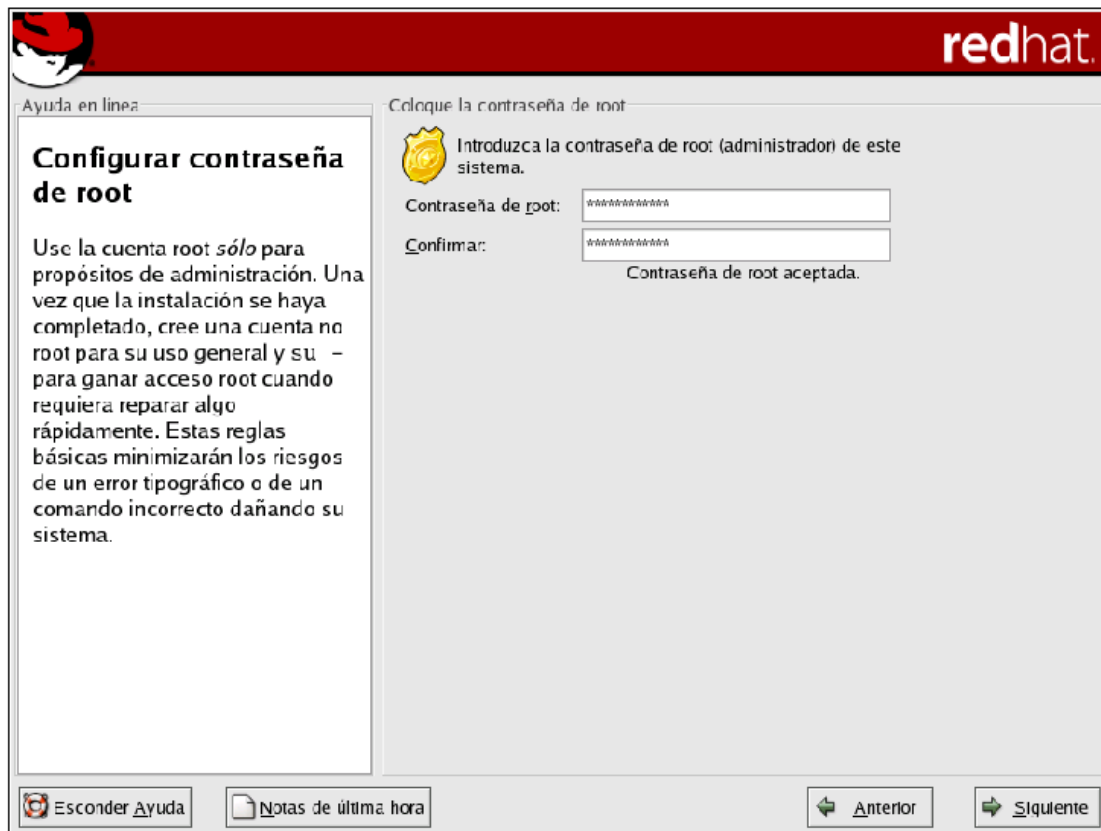


Figura 22. Introducción de contraseña de administrador.

Utilice la cuenta de root tan sólo para la administración de su sistema. Cree una cuenta que no sea root para uso general y ejecute su - para actuar como root cuando necesite configurar algo de forma rápida. Estas normas básicas minimizarán las posibilidades de que un comando incorrecto o de un error de tipografía pueda dañar su sistema. Para convertirse en root, teclee su - en el intérprete de comandos de la shell en una ventana de terminal y, a continuación teclee intro. Luego, introduzca la contraseña de root y pulse intro.

La contraseña de root debe de tener al menos seis caracteres y no aparecerá en la pantalla cuando la teclee. Deberá introducirla dos veces; si las dos contraseñas no coinciden, el programa de instalación le pedirá que las vuelva a introducir. Para cambiar su contraseña de root después de que haya completado la instalación, utilice la Herramienta de contraseña root. Escriba el comando `redhat-config-rootpassword` en un intérprete de comandos de la shell para lanzar la herramienta

de contraseña root. Si no es root, se le indicará que introduzca la contraseña de root para continuar.

## Selección de grupos de paquetes

Tras haber seleccionado sus particiones y haberlas configurado para su formateo, se está preparado para la instalación de los paquetes. Por ejemplo, si está realizando una instalación de tipo Escritorio Personal, verá una pantalla similar a la figura siguiente.

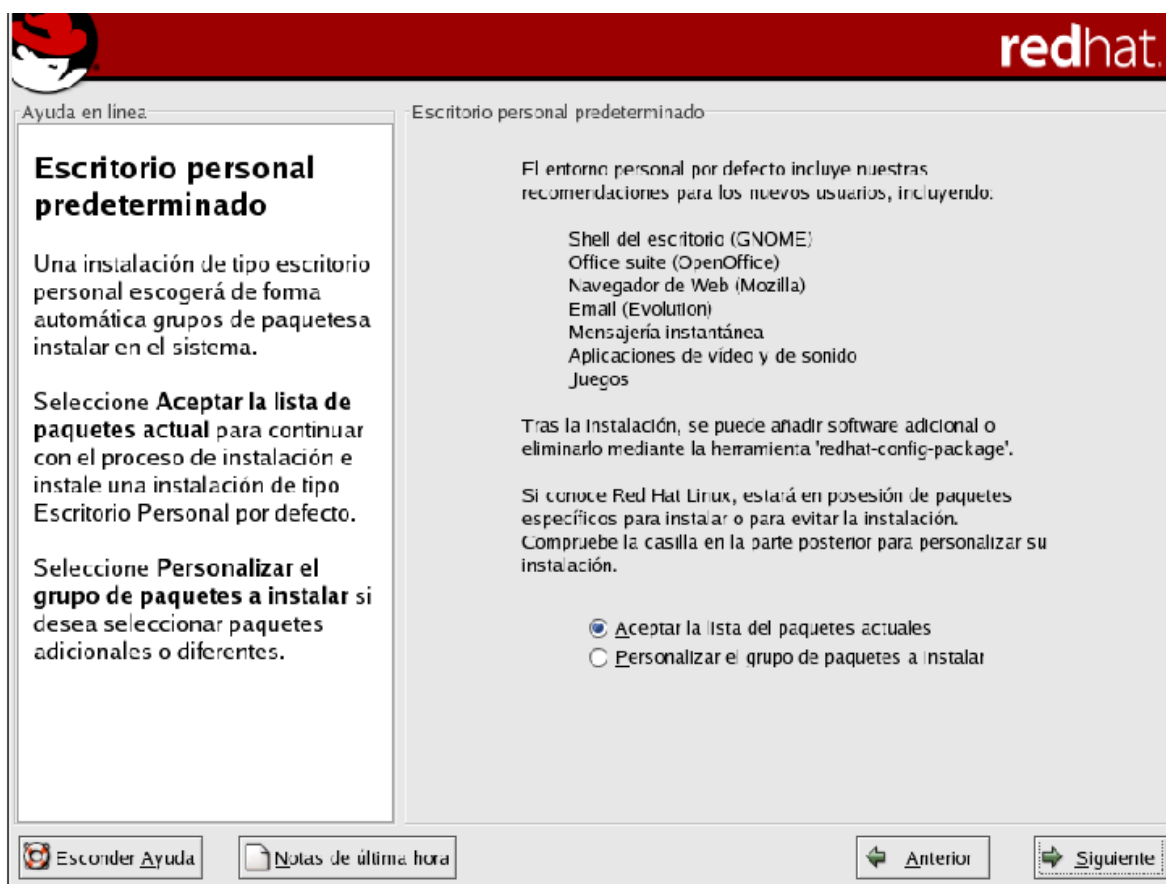


Figura 23. Selección de paquetes.

Para seleccionar paquetes individualmente, compruebe la casilla de verificación personalizar el conjunto de paquetes a instalar. Se seleccionará grupos de paquetes, los cuales agrupan componentes de acuerdo a una función (por ejemplo, Sistema X Window y Editores), paquetes individuales, o una combinación de los dos.

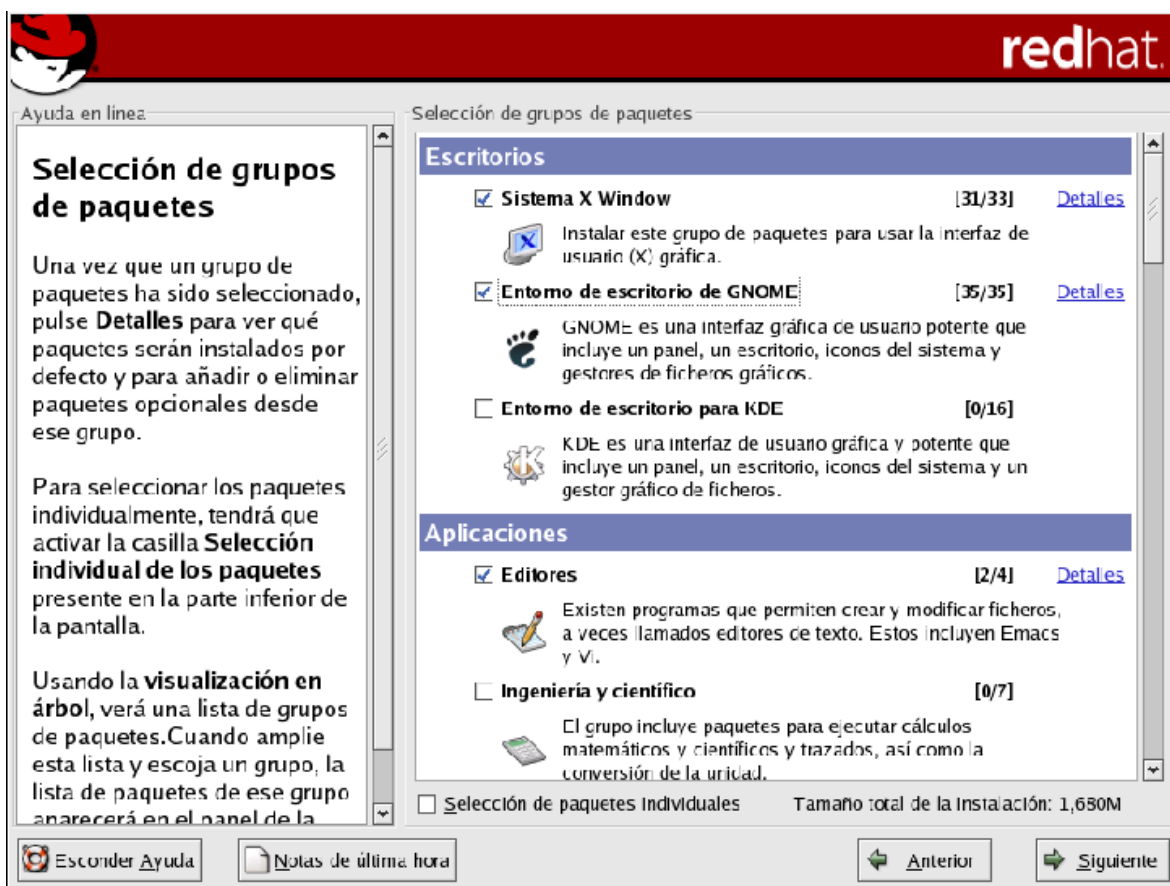


Figura 24. Selección de paquetes individuales.



## Instalación de paquetes

En este momento, no se podrá hacer nada hasta que todos los paquetes hayan sido instalados. La rapidez de este proceso dependerá del número de paquetes que se hayan seleccionado y de la velocidad de la computadora.



Figura 25. Instalación de paquetes de Red Hat.

## Creación de un disquete de arranque

Para crear un disco de arranque, introduzca un disco en blanco, formateado en su unidad de disco y haga clic en "Siguiente". Se recomienda que se cree un disquete de arranque, un disco de arranque permitirá arrancar de forma adecuada el

sistema Red Hat Linux. Tras un pequeño tiempo de espera, el disquete de arranque estará creado; sáquelo de la disquetera. Si no desea crear un disco de arranque, asegúrese de que selecciona la opción adecuada antes de pulsar “Siguiente”.

## Configuración de la tarjeta de vídeo

El programa de instalación a continuación proporcionará una lista de tarjetas de vídeo entre las que escoger. Si la tarjeta de vídeo no aparece en la lista, X puede que no la soporte. No obstante, si posee conocimiento técnico sobre su tarjeta, puede escoger tarjeta no listada e intentar configurarla al hacer corresponder su chipset de tarjeta de vídeo con uno de los servidores X disponibles.

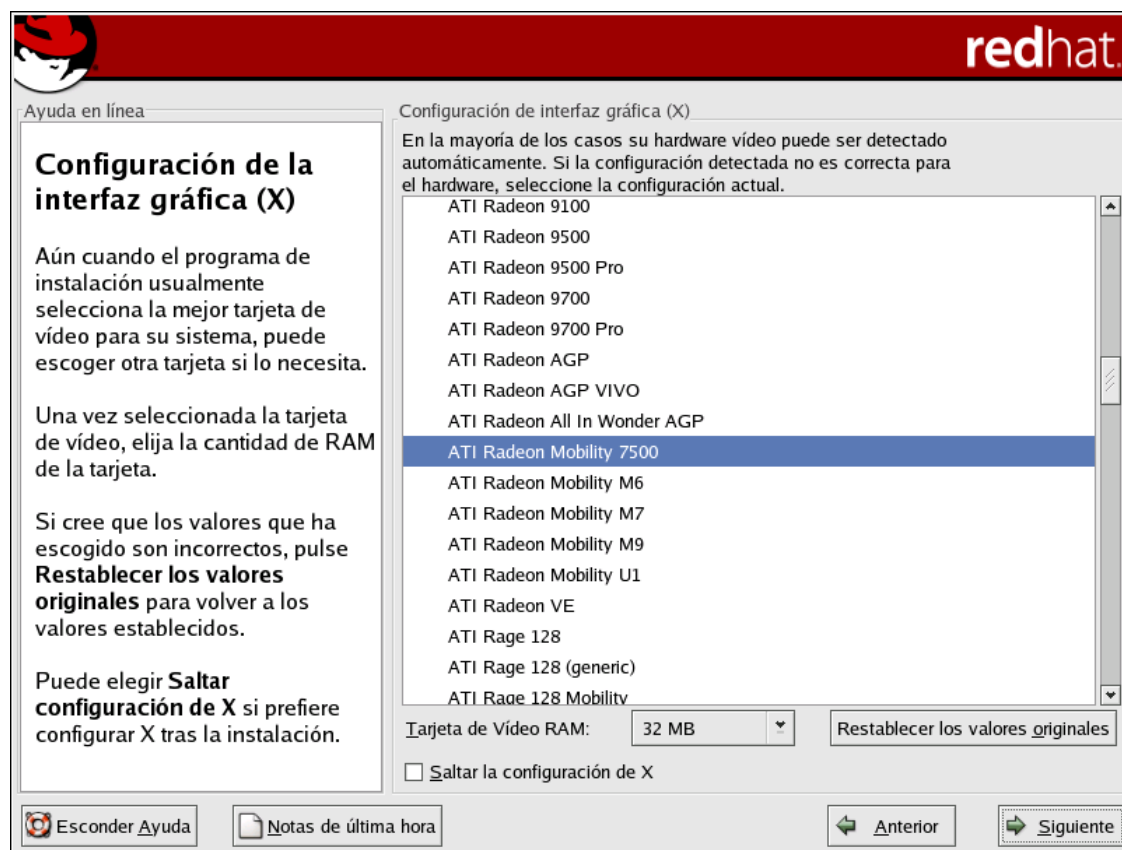


Figura 26. Selección de la tarjeta de video.

## **Fin de la instalación**

El programa de instalación pedirá que prepare el sistema para reiniciarse. No olvidar sacar cualquier disco de las disqueteras y CD de la unidad de CD-ROM.)

Si no se tiene un gestor de arranque instalado y configurado, necesitará usar el disco de arranque que ha creado durante la instalación. Después de que la secuencia de encendido se haya terminado, debería visualizar el intérprete de comandos del gestor de arranque gráfico en el que puede hacer cualquiera de las siguientes cosas:

Teclear intro: se reiniciará la entrada de inicio por defecto.

Seleccionar una etiqueta de arranque seguida de intro: provocará que el gestor de arranque inicie el sistema operativo correspondiente a la etiqueta de arranque. (Pulse [?] o [Tab] en el intérprete de comandos del cargador de arranque en modo texto para una lista de etiquetas de arranque válidas.)

No hacer nada: tras un período de espera, inicializará la primera partición automáticamente. Se observará una o más ventanas de mensajes, también debería ver un intérprete de comandos login: o una pantalla gráfica de login.

## **Instalación y configuración básica de la Honeynet**

La instalación de la honeynet comprende en gran medida de una etapa previa que es la instalación del sistema vmware en donde radicarán los honeypots, por tal motivo se deben de crear varias instancias de sistemas virtuales. En el sistema principal radicará en honeywall, que es una de las piezas principales para nuestra red honeynet. En la figura 27 se podrá recordar del sistema de honeynet y de cuales elementos está conformada.

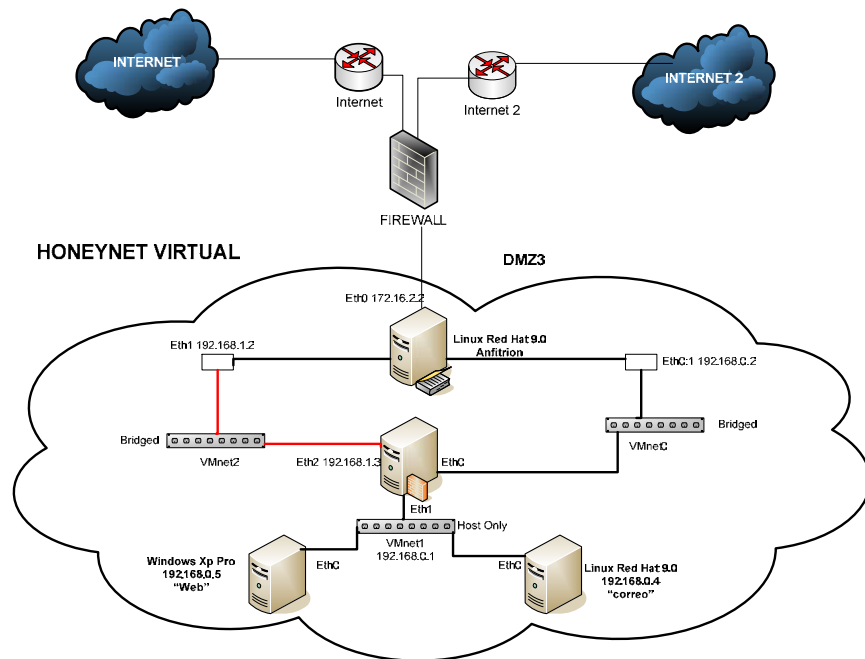


Figura 27: Diseño de la Honeynet Virtual-DMZ

## Instalación de VMWare

Sobre el aplicativo de Vmware se deberá de crear maquinas virtuales utilizando el “virtual Machine Control” para realizar los ajustes sobre los adaptadores Ethernet. Seleccionar “New Virtual Machine” como aparece en la siguiente figura 28.

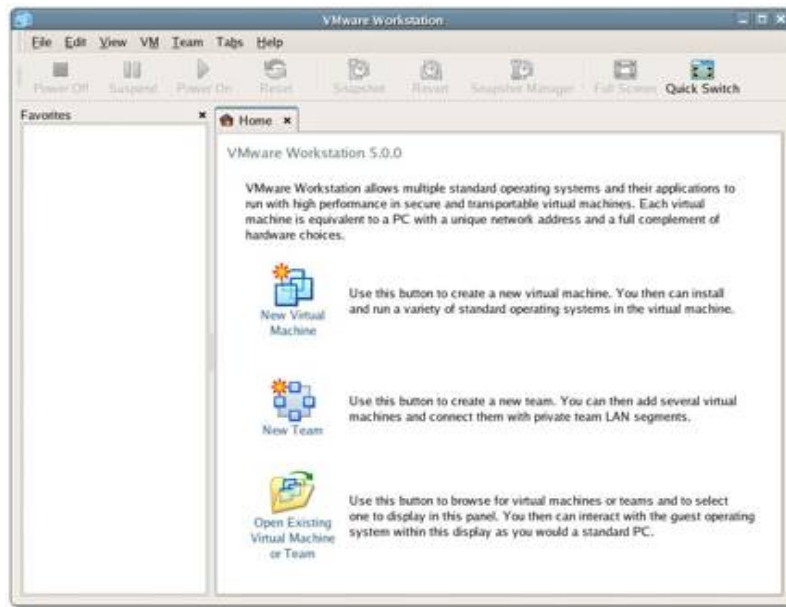


Figura 28. Selección de la nueva máquina virtual.

Seleccionar “Custom” para la configuración de la maquina virtual, ver figura 29. Esto permitirá realizar la creación de la maquina virtual con dispositivos adicionales con opciones específicas de configuración. Seleccionar seguidamente “Next”.



Figura 29. Selección de la configuración “Custom”.

Seleccionar “New – Workstation 5” para realizar el formato de la maquina virtual, en la cual hay varias características disponibles para la parte de la configuración. Seleccionar seguidamente “Next”.

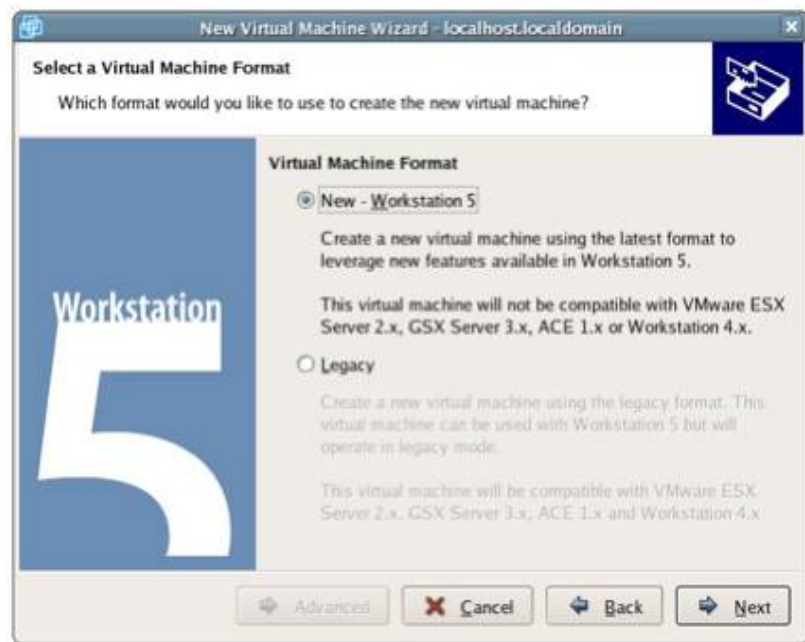


Figura 30. Selección de la creación de nueva estación de trabajo.

Luego hay que realizar la selección del sistema operativo huésped, para el caso en particular del prototipo se debe de seleccionar Linux con Red Hat 9. Seleccionar seguidamente “Next”.

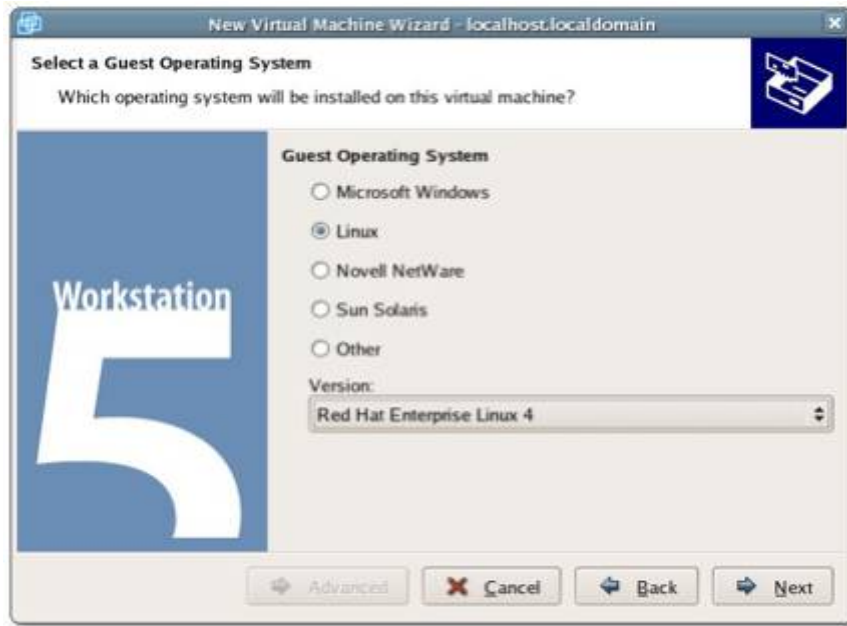


Figura 31. Selección del sistema operativo huésped.

En la selección del nombre de la maquina virtual se deberá de poner el nombre del sistema a realizar, en este caso en se nombrará como “Honeywall”. Seleccionar seguidamente “Next”.



Figura 32. Selección del nombre de la maquina virtual

Se asignará por lo menos 256 MB de memoria para la maquina virtual de honeywall aunque 512 MB que es el recomendado. Seleccionar después “Next”.



Figura 33. Selección de espacio de memoria.

Seleccionar “Use bridged networking” para la conexión de red. Se realizará la adición de dos o más “bridged and host only network connections” después de completar la instalación guiada con el fin de adicionar todos los dispositivos requeridos para el buen funcionamiento. Seleccionar seguidamente “Next”.



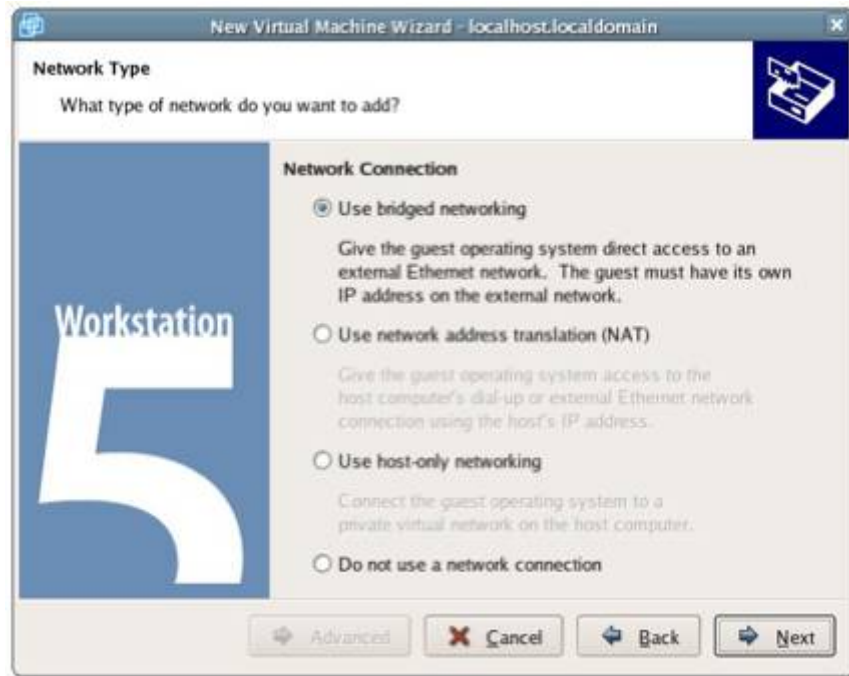


Figura 34. Selección de tipo de tarjeta de red.

Se deberá de seleccionar el tipo de adaptador de entrada y salida. El Honeywall puede soportar controladoras de disco SCSI e IDE. Seleccionar para este caso SCSI LSI. Presionar seguidamente “Next”.

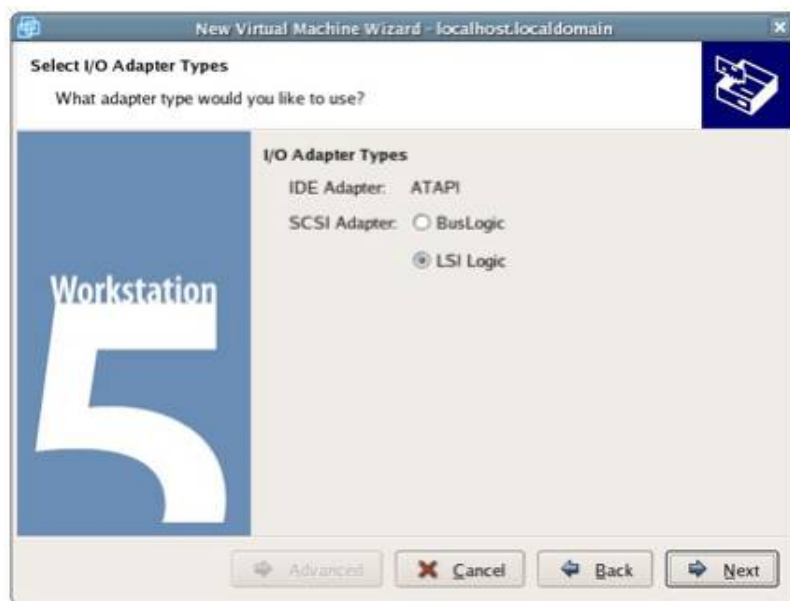


Figura 35. Selección de adaptadores de entrada / salida.

Seleccionar “Create a new virtual disk” para crear un disco virtual del disco físico, es decir se estará asignando un espacio físico a la unidad virtual. Presionar seguidamente “Next”.



Figura 36. Selección de disco virtual.

Seleccionar el tipo de dispositivo para el disco virtual. Para este caso seleccionar IDE y seguidamente “Next”.

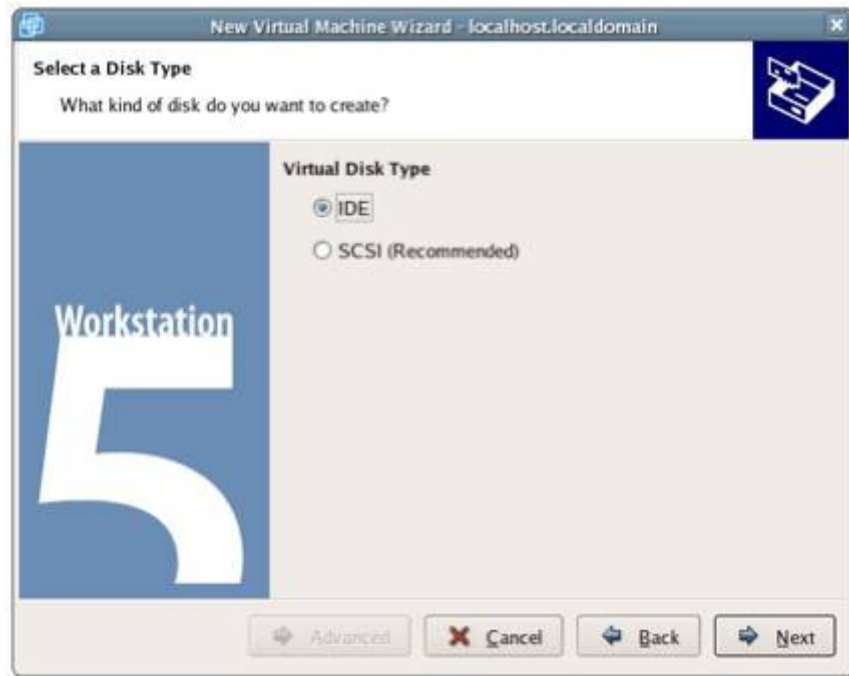


Figura 37. Selección del tipo de disco virtual.

Seleccionar la capacidad del disco virtual. Para propósitos del prototipo seleccionar la capacidad de 4 GB que es la capacidad mínima para la instalación del honeywall. Siempre es recomendado mayor capacidad de disco. Presionar seguidamente "Next".



Figura 38. Selección de la capacidad de disco virtual.

Luego se especificará la locación en donde se guardará la información. Se puede dejar la ruta o la locación que trae por defecto pero si es requerido seleccionar otra locación se debe de especificar en este paso. Seguidamente presionar “Finish”, con este paso se finaliza la instalación de forma guiada.



Figura 39. Selección de la locación de los archivos.

La próxima pantalla que se desplegará es el resumen de la información de la configuración de maquina virtual, terminando así el asistente la instalación de forma guiada.



Figura 40. Despliegue normal de vmware.

Se utilizará el panel de control de la maquina virtual para realizar los cambios de edición del Honeywall. En este caso en particular se adicionará adaptadores de red virtuales y realizar la conexión hacia el “Network Bridged” denominado “VMnet0” y los “Host-only Networking” los cuales se denominan VMnet1 respectivamente. Finalmente la configuración se observará como en la figura 41.

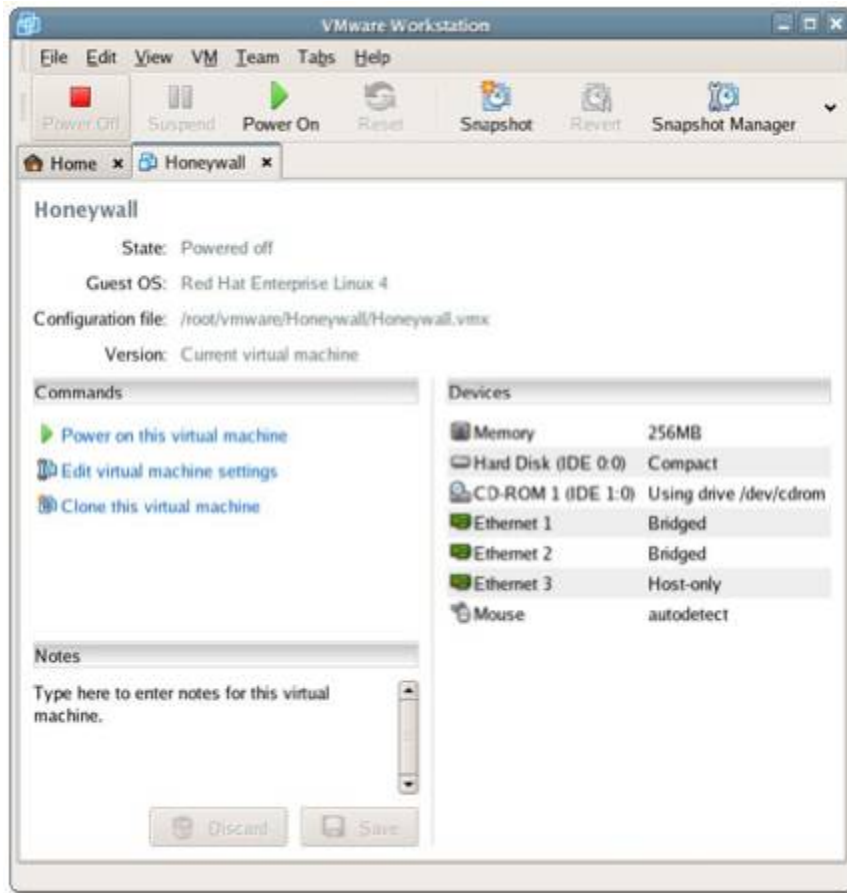


Figura 41. Configuración de Vmware.

Se deberá de crear dos maquinas virtuales para los otros dispositivos con “host-only networking”. Después de desarrollado esto se tendrá las máquinas virtuales necesarias, listas para instalarse el sistema operativo huésped. Luego de eso se deberá de reiniciar la computadora con la maquina virtual deseada con la media del sistema operativo según los pasos del manual correspondiente y realizar la instalación del mismo. Configurar estas maquinas virtuales con una dirección IP las cuales serán a las IP de la computadoras a las cuales los atacantes tratarán de violar.

## Instalación y configuración del Honeywall

### Arranque

Se deberá de inicializar a través de la maquina virtual designada para el honeywall y luego arrancar con el disco de Honeywall (adicionado a esta literatura). El proceso de inicialización deberá de desplegar una pantalla como el de la figura 42 del proyecto de honeynet. En este punto el sistema entrará en una pausa momentánea, al presionar seguidamente de esta pausa el sistema sobrescribirá toda su información y la instalación en la información que contenga el disco duro y procederá a realizar el proceso de instalación. Presionar “intro” para realizar la instalación.



Figura 42. Pantalla de bienvenida de la instalación de honeynet.

Una vez que la instalación comienza este será un proceso automático y no es necesario realizar algún tipo de interacción a partir de este punto.

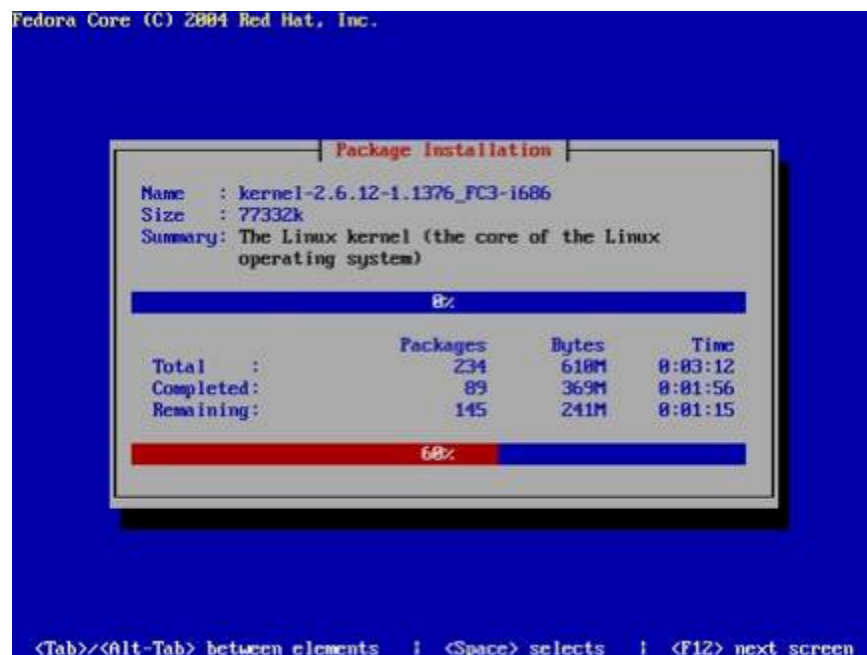


Figura 43. Instalación de honeynet.

Después de que la instalación ha sido completada, el sistema automáticamente reiniciará la maquina. Uno de los parámetros que se deberá de cambiar en el mismo momento de reiniciar es cambiar la secuencia de búsqueda del sistema siendo el disco duro el primero en el cual buscará el sistema y luego en el CD-ROM. Si no se logrará realizar la modificación a tiempo se debe de retirar el disco de instalación para evitar un nuevo ciclo de instalación.

Después de que el sistema haya reiniciado, la instalación ha sido completada y deberá de presentar el prompt de la línea de comando. A este punto se podrá realizar un login y comenzar con el proceso de la configuración estándar. El honeywall viene con dos cuentas del sistema por defecto (roo y root) y ambas poseen el mismo password que es honey. No será posible hacer una autenticación o un login como root si no que deberá de acompañar con roo su- .



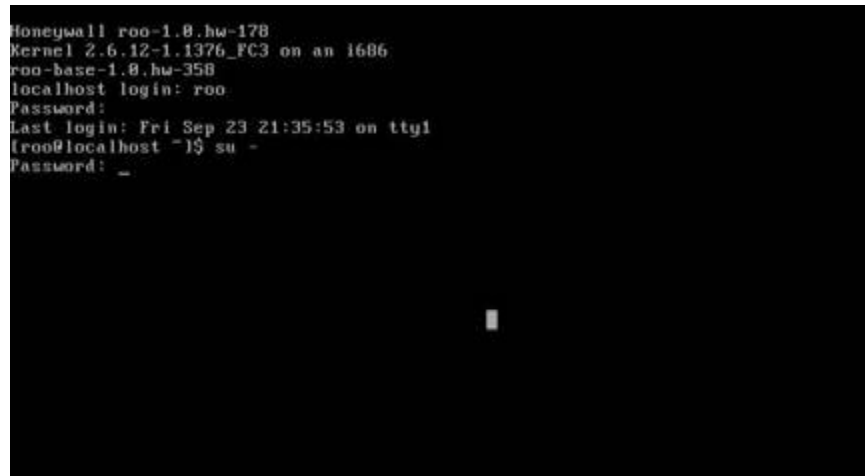


Figura 44. Pantalla de autenticación.

Mensaje después de la autenticación “When you login to Honeywall for the first time, it gives an alert saying that your Honeywall is not yet configured and recommends using the Honeywall Configuration option on the main menu”. Seleccionar **OK** para proceder.



Figura 45. Pantalla después de autenticación.

## Configuración del Honeywall

En el menú principal del honeywall, seleccionar la opción 4, configuración de honeywall y seleccionar OK para proceder.



Figura 46. Selección de la configuración del honeywall.

Luego del inicio de la pantalla de inicio de configuración aparecerá un mensaje de la limitación de la responsabilidad. Hay riesgos involucrados en el Honeynet Virtual, así como el despliegue Honeynet. Como se está realizando una Honeynet Virtual, puede haber riesgos involucrados en el mismo. Si un atacante es capaz de comprometer el sistema operativo sobre el que se está ejecutando software de virtualización, él sería capaz de controlar todo el sistema. En segundo lugar, si un atacante compromete el sistema en su Honeynet Virtual, que puede llegar a detectar que el sistema está funcionando en un ambiente virtual. Leer detenidamente y haga clic en Sí para el reconocimiento.

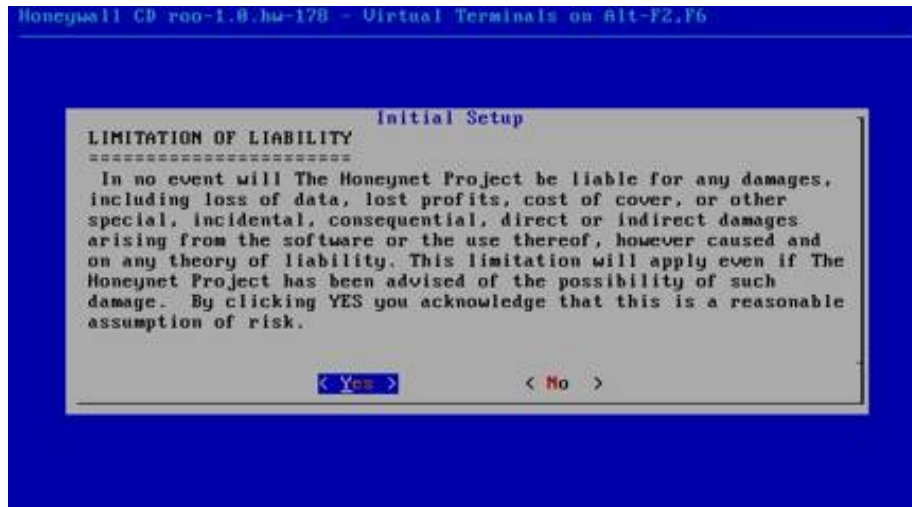


Figura 46. Mensaje de la limitación de la responsabilidad.

Seguidamente se desplegará la pantalla del menú del método de la configuración el cual permite seleccionar el método de instalación. Ofrece tres métodos para configurar la Honeywall, el primero de ellos es el de disco Floppy el cual contendrá la configuración (honeywall.conf) en la unidad de disquete. Este método es útil y más rápido para el despliegue de gran número de Honeywalls.

El método "Defaults" restaura el Honeywall a la configuración que trae por defecto de fábrica. Para ello se utiliza el valor de honeywall.conf en el fichero de configuración que viene con el sistema. El método de entrevista, realizará una serie de preguntas para configurar la Honeywall. Si se está configurando Honeywall por primera vez, se recomienda utilizar esta opción. Para efectos de esta instalación se seleccionará entrevista y pulse intro.



Figura 47. Selección de la configuración de la forma tipo entrevista.

Luego se desplegará un mensaje de configuración inicial, presionar intro para proceder.



Figura 48. Mensaje de la configuración inicial.

Introducir el rango de las direcciones IP "pública" para los honeypots. Esta será la identificación en el cual el atacante conocerá a los sistemas sistema. Presionar intro para proceder.



Figura 49. Configuración el rango de las direcciones IP de los honeypots.

Seleccionar la red y la máscara de subred en donde estarán los honeypots. Esta notación esta en tipo barra y CIDR (Classless Inter-Domain Routing). Presionar seguidamente intro para proceder.



Figura 50. Configuraciones de dirección IP y mascara de red.

Introducir la dirección IP en donde termina la subred o como mejor es conocida como la dirección de “broadcast”. Para en este caso en particular se está haciendo referencia a la dirección 10.0.0.255 que es la última dirección de toda esa subred según la nomenclatura de barra 24 introducida anteriormente. Presionar intro seguidamente para proceder.



Figura 51. Configuración de dirección de broadcast.

Seleccionar ok para proceder con la configuración de la administración remota.



Figura 52. Finalización de la configuración inicial.

Seleccionar “Yes” para realizar la configuración de la interfaz gráfica de administración.

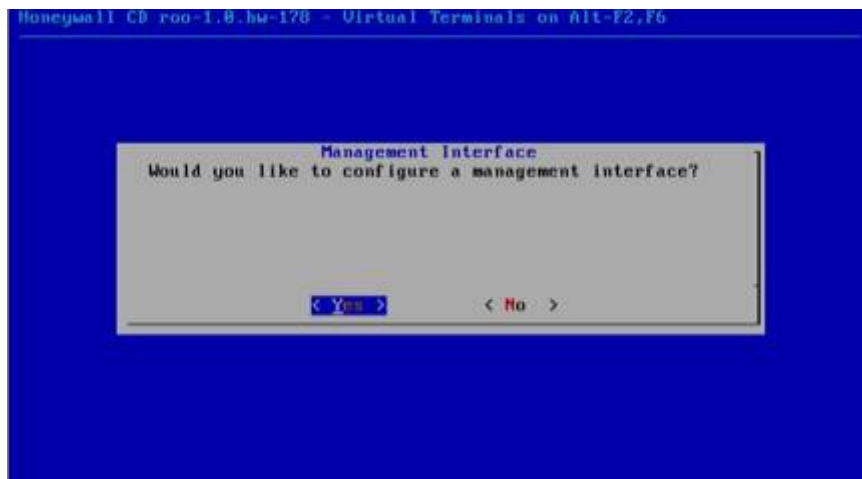


Figura 53. Selección de configuración de interfaz gráfica.

El sistema Honeywall detectará automáticamente la interface a la cual ha sido habilitada para en este caso en particular se ha detectado la eth2 para la administración. Presionar seguidamente intro en “ok” para proceder.

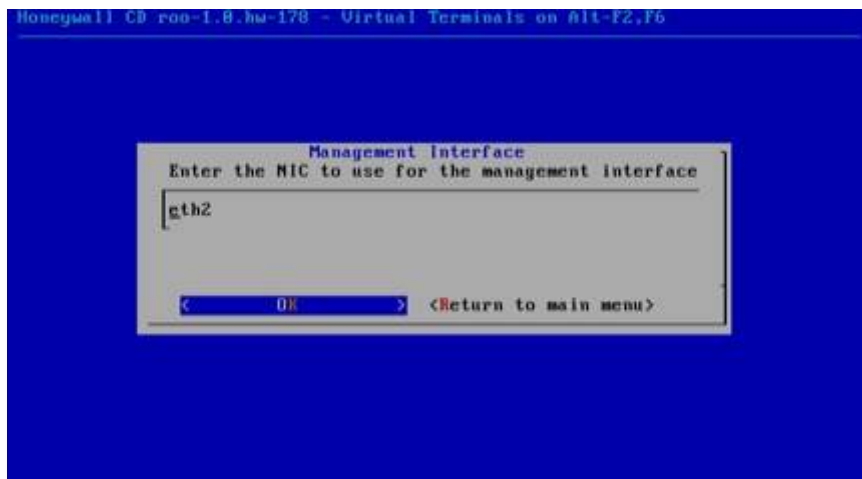


Figura 54. Selección de interface de red por la cual se realizará la administración.

Habrà que seleccionar la dirección IP con la cual se buscarà la interfaz de administración e introducirla en el valor que solicita, para en este caso en

particular se está introduciendo la 10.10.10.66 la cual será escrita en el buscador de internet para habilitar la administración por esta vía. Presionar intro en “ok” para proceder.



Figura 55. Dirección IP de la interfaz gráfica.

Seleccionar la red y la máscara de subred en donde estarán los honeypots. Esta notación esta en tipo barra y CIDR (Classless Inter-Domain Routing) notation. Presionar seguidamente intro para proceder.



Figura 56. Mascara de la interfaz gráfica.



Introducir la puerta de enlace “default gateway” de la interfaz de administración y presionar intro en ok.



Figura 57. Puerta de enlace de la interfaz gráfica

Introducir el dominio de DNS de la interfaz de administración y presionar intro en ok.



Figura 58. DNS de la interfaz gráfica

Introducir la dirección IP del servidor del dominio de DNS de la interfaz de administración y presionar intro en ok.



Figura 59. Dirección del servidor DNS.

Seleccionar "Yes" para activar la interfaz de administración.

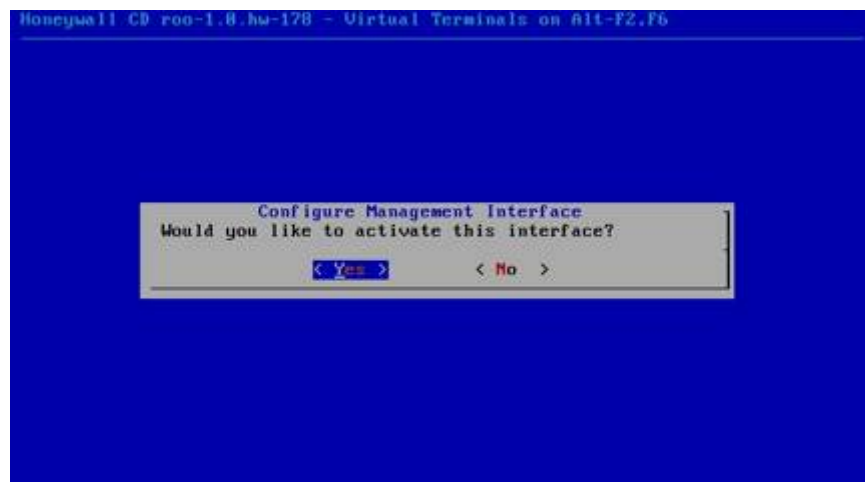


Figura 60. Activación de la interface.

Seleccionar "Yes" para que la interfaz de administración arranque en la próxima sesión o iniciación del sistema.

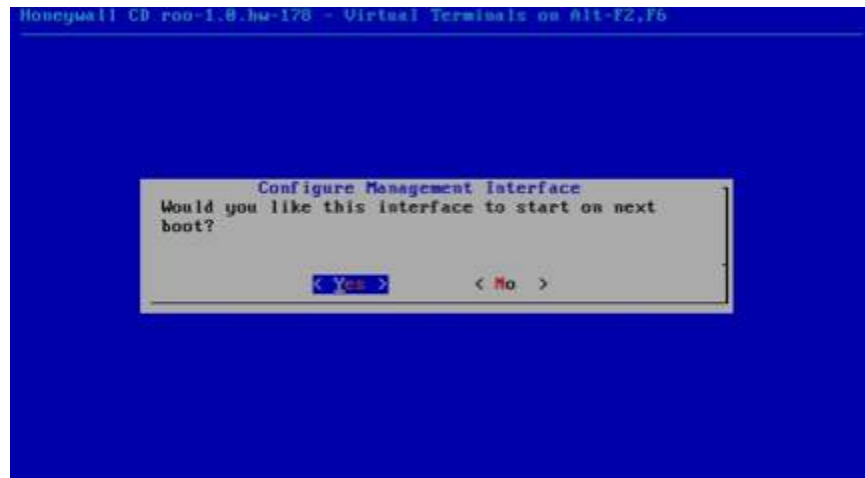


Figura 61. Solicitud de reinicio.

Seleccionar "Yes" para realizar la configuración de SSH.

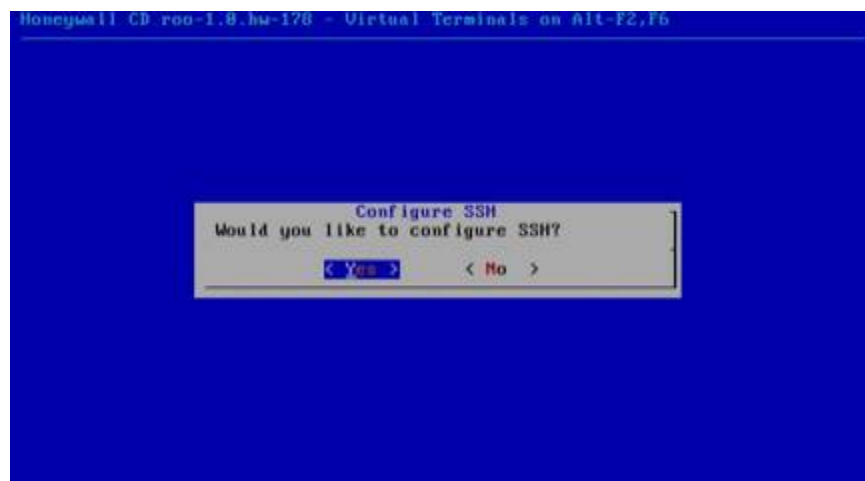


Figura 62. Configuración de SSH.

Introducir el Puerto en el cual se quiere realizar o se quiere escuchar el tráfico de SSH, presionar intro en ok seguidamente. El valor de la configuración por defecto es el puerto 22 para este aplicativo.

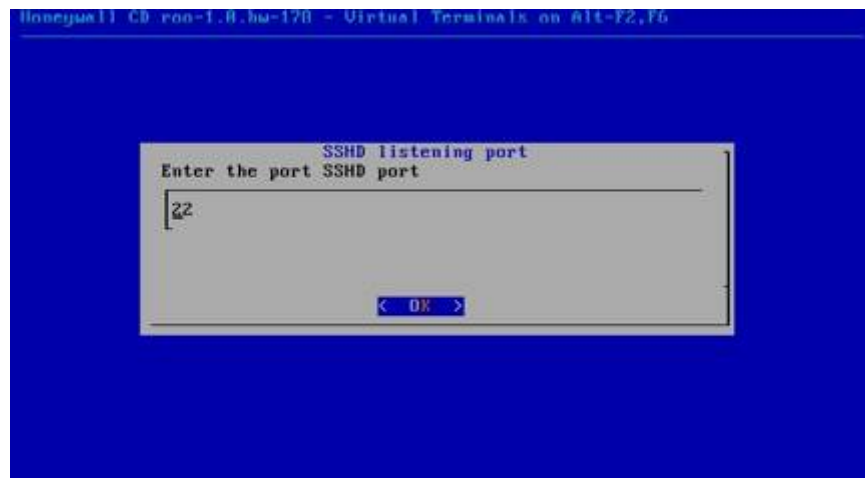


Figura 63. Selección de puerto para SSH.

Introducir un usuario con el cual remotamente se realizará la autenticación, presionar intro en ok seguidamente.



Figura 64. Selección de usuario.

Seleccionar "Yes" para realizar el cambio de la contraseña (password) del nuevo usuario.

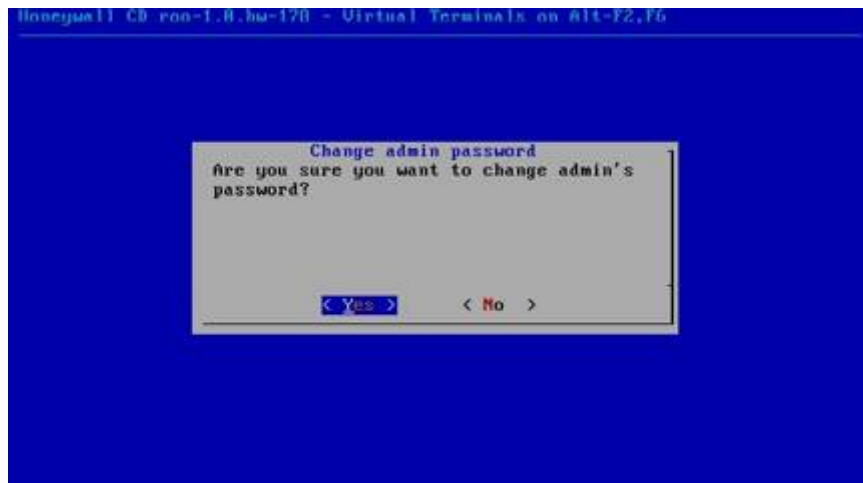


Figura 65. Selección de contraseña.

Introducir la nueva contraseña y presionar en ok. El sistema validará la contraseña preguntando por ella para lo cual se debe de digitar nuevamente. Presionar intro en ok para proceder después de ingresada.



Figura 66. Ingreso de contraseña.



Figura 67. Mensaje de contraseña cambiada.

Preguntará el sistema si se desea cambiar la contraseña de root, para este ejemplo en particular seleccionar “Yes” para realizar esta tarea.



Figura 68. Mensaje de cambio de contraseña de root.

Introducir la nueva contraseña de root y seleccionar ok para continuar. El sistema validará la contraseña preguntando por ella para lo cual se debe de digitar nuevamente. Luego de eso seleccionar ok para proceder.



Figura 69. Confirmación de ingreso de contraseña.



Figura 70. Contraseña cambiada.

Luego de este paso, el sistema preguntará si se desea habilitar la interfaz de administración del honeywall que se denomina “Walleye” para permitir el análisis de datos y la administración del honeywall. Seleccionar “Yes” para proceder a este paso.

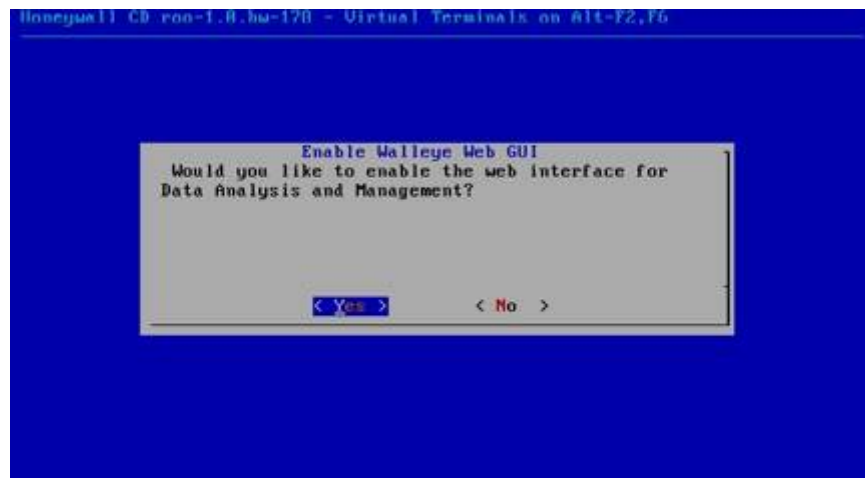


Figura 71. Habilitación de la interfaz de administración

El siguiente paso es si se quiere seleccionar el firewall interno para restringir las conexiones. Seleccionar "No" para omitir este paso para este ejemplo en particular.

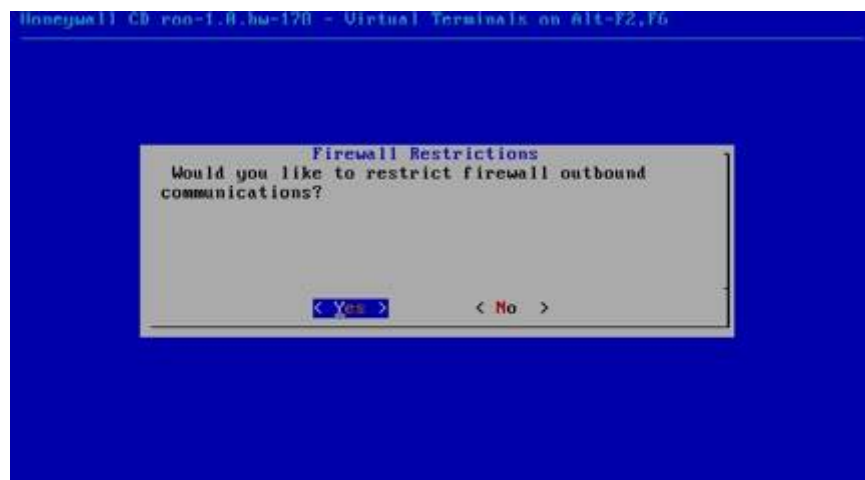


Figura 72. Habilitación de firewall.

El siguiente paso desplegará el mensaje de configuración inicial finalizada a lo cual se debe de seleccionar en ok para finalizar esta parte de la instalación.





Figura 73. Configuración de firewall.

## Configuración de limitaciones de las conexiones de salida

Se ha permitido todo el tráfico entrante al honeypot, pero limitando las conexiones de salida. Por lo tanto, una vez que un límite haya sido superado cualquier nuevo intento de conexión será bloqueado como prevención que el sistema sea dañado. La opción de limitación de conexiones da 5 posibles formas o escalas para limitar las conexiones salientes.

Segundo: por escala de tiempo en segundos, esta será aplicada una vez que sea superado el valor de la escala.

Minuto: por escala de tiempo en minutos, esta será aplicada una vez que sea superado el valor de la escala.

Hora: por escala de tiempo en horas, esta será aplicada una vez que sea superado el valor de la escala.

Día: por escala de tiempo en días, esta será aplicada una vez que sea superado el valor de la escala.

Por ejemplo si establece TCP limitar a 9 saliente de conexiones por hora. Esto permitirá a un atacante hacer 9 TCP en las conexiones de salida de una hora y cuando se llega al límite, no será capaz de hacer más conexiones. El límite será reajustado después de una hora. Escoger e introducir la escala y presionar intro en ok para proceder con la instalación y configuración.



Figura 75. Opción de limitación de conexiones

Introducir el número de conexiones salientes del protocolo TCP y luego seleccionar ok presionando intro sobre esta opción.

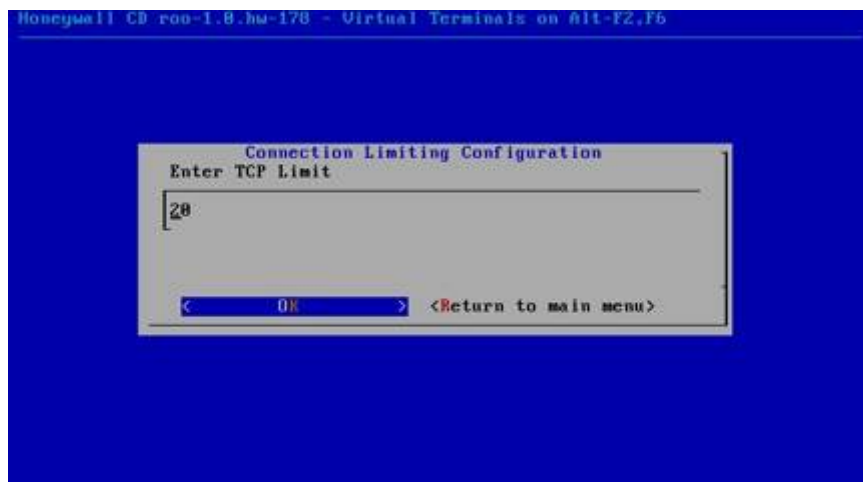


Figura 76. Opción del puerto de limitación de conexiones

Introducir el número de conexiones salientes del protocolo UDP y luego seleccionar ok presionando intro sobre esta opción.

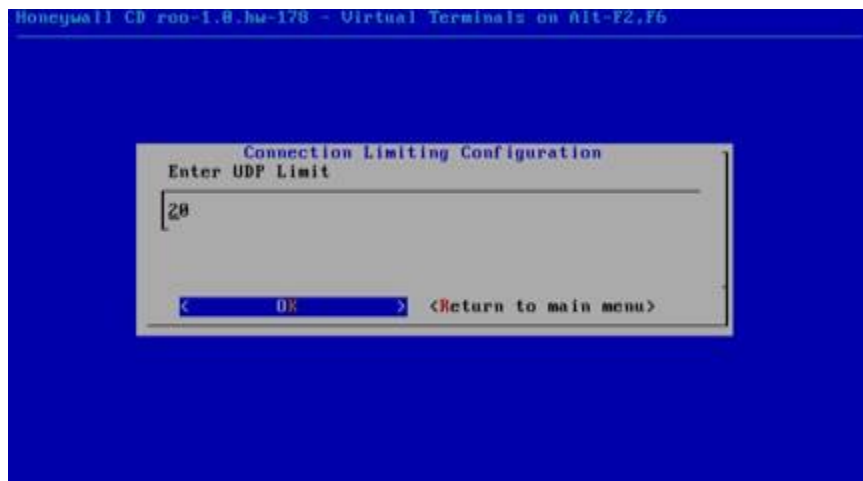


Figura 77. Opción del puerto de limitación de conexiones

Introducir el número de conexiones salientes del protocolo ICMP y luego seleccionar ok presionando intro sobre esta opción.

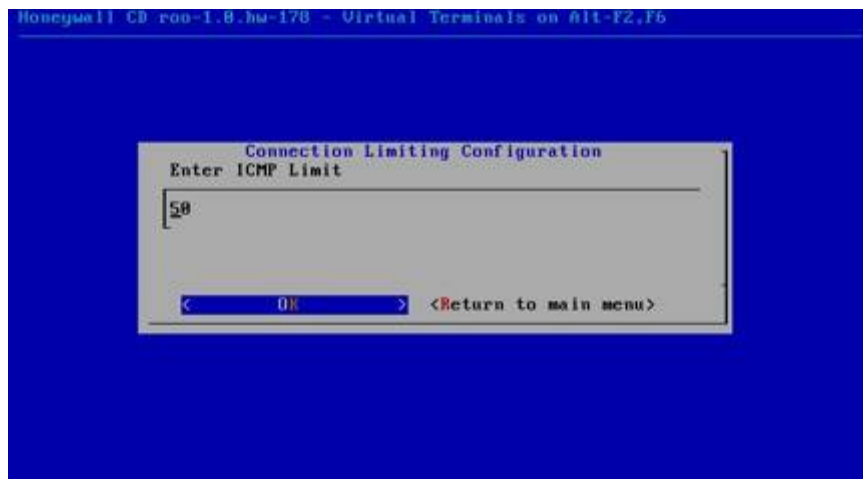


Figura 78. Opción del puerto de limitación de conexiones

Seleccionar el límite de otros tipos de protocolo y ICMP y luego seleccionar ok presionando intro sobre esta opción.

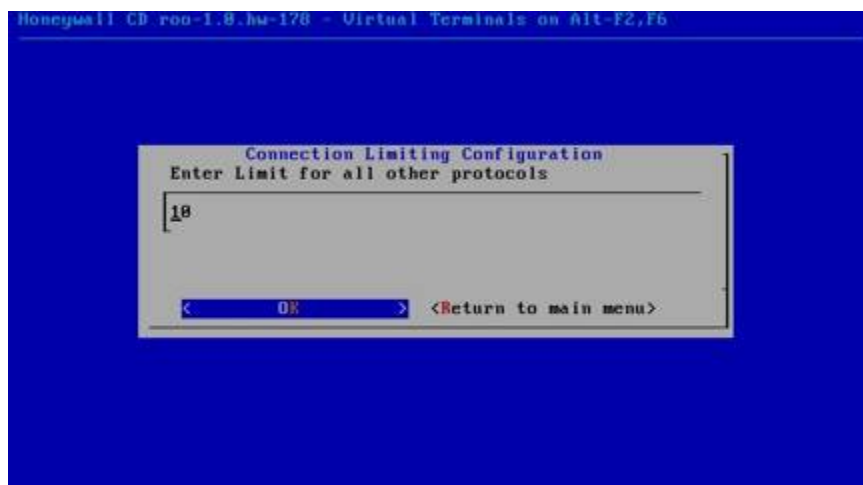


Figura 79. Opción del puerto de limitación de conexiones

## Configuración del Snort Inline

El Snort Inline permite realizar desechar, rechazar y reemplazar ataques conocidos mediante patrones llamados firmas. Seleccionar Yes para configurar para que el firewall envíe paquetes al snort inline.

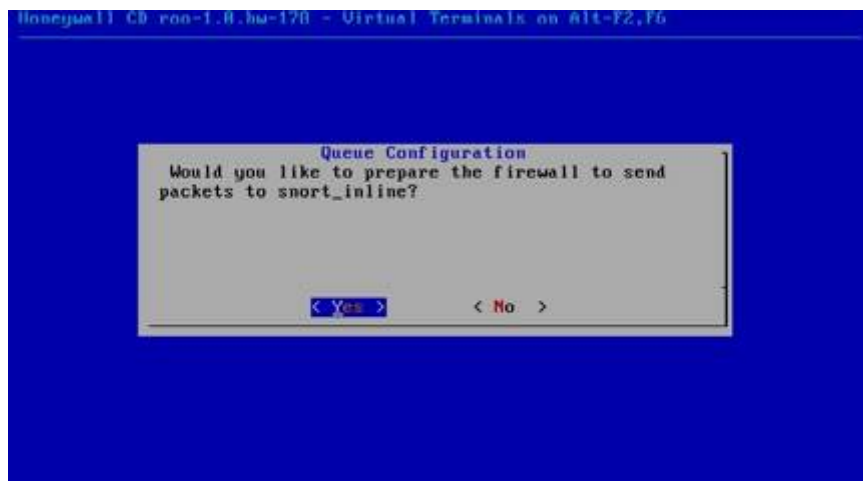


Figura 80. Configuración de snort inline.

Luego de haber realizado la selección del envío de paquetes del firewall al snort, se debe de seleccionar el set de reglas o de acciones que se desea que el snort haga, para este caso en particular de configuración se escogerá desechar posicionándose en “drop” y seguidamente intro en ok.



Figura 81. Configuración de opción “drop”.

Se deberá de realizar la configuración del filtrado. Honeywall ofrece varias características de capacidad de control de datos, entre los que podemos mencionar.

Black list – Lista negra, desechará las direcciones IP que se encuentra acá y los bloqueará sin ningún tipo de log en el sistema.

White list – Lista blanca, permite las direcciones IP que se encuentran acá pero con log del sistema.

Fence list – Lista de protección o de barrera, protege las direcciones IP y bloquea desde el honeypot para que se tenga acceso a la misma.

Roach motel – Sin traducción literal, pero hacienda referencia a una trampa para matar cucarachas. Para este término en particular deshabilita en ese momento de

ataque todo el tráfico saliente del honeypot. Se seleccionará la opción de black-list y presionar ok. Luego se debe de escribir el nombre del archivo que contiene esto, el cual es “blacklist.txt” y presionar intro en ok.

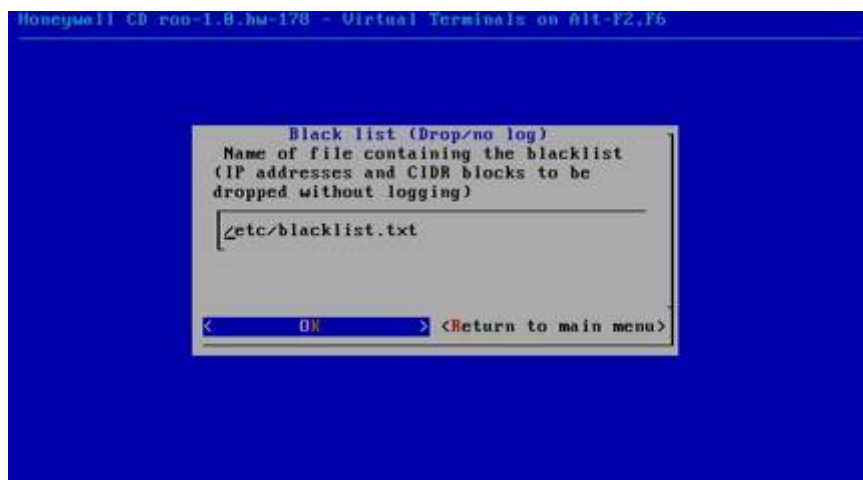


Figura 82. Selección de archivo de blacklist.

Para seleccionar la opción de white-list se debe de escribir el nombre del archivo que contiene esto, el cual es “whitelist.txt” y presionar intro en ok.



Figura 82. Selección de archivo de whitelist.

Seleccionar “Yes” para habilitar la “black-list” y la “white-list” para realizar el filtrado.

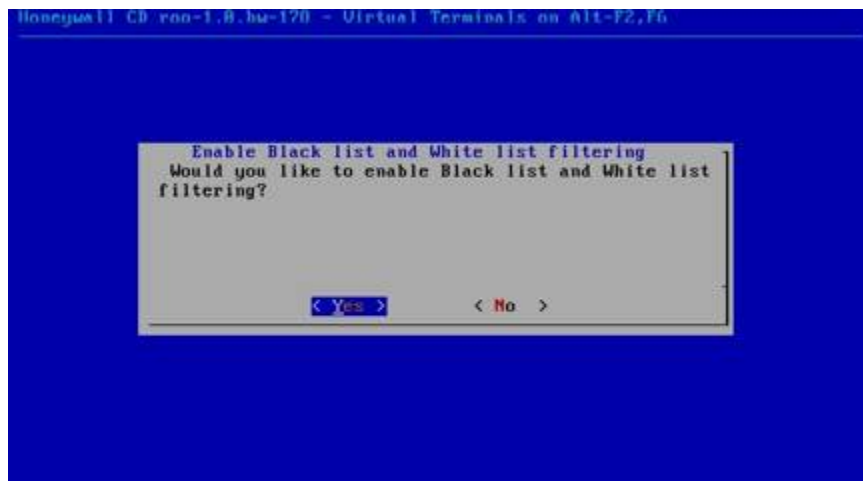


Figura 83. Habilitación de las listas.

Para seleccionar la opción de fence-list se debe de escribir el nombre del archivo que lo contiene, el cual es “fencelist.txt” y presionar intro en ok.



Figura 84. Selección de archivo de fencelist

Para este caso en particular no se habilitará esta característica, por lo que se debe de seleccionar no y presionar intro.



Figura 85. Selección de filtrado de fancelist.

Tampoco se habilitará la característica de Roach motel, por lo que se deberá de seleccionar No.



Figura 86. Selección de filtrado de "Roach Motel"



Seleccionar ok para proceder la configuración de DNS en el honeypot.



Figura 87. Configuración de DNS.

La limitación de DNS permitirá configurar los DNS para su acceso al honeypot. Esto ayudará a no hacer conexiones ilimitadas hacia cualquier lado o dispositivo desde el honeypot. Para este caso en particular se permitirá para que se tenga acceso ilimitado en el DNS. Seleccionar "Yes" y presionar intro.

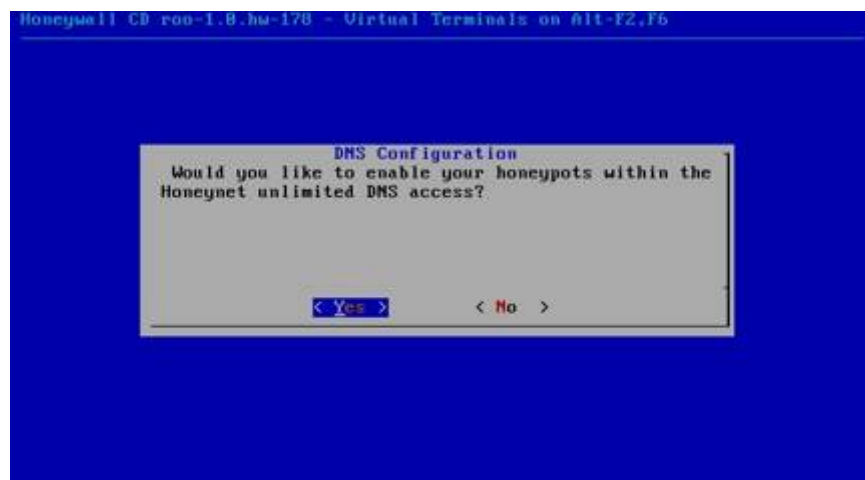


Figura 88. Selección de habilitación de DNS.

Se dejará que los honeypots no tengan restricciones de acceso externo ilimitado al servidor de acceso de DNS. Seleccionar no y presionar intro.



Figura 89. Configuración de DNS.

Escribir la lista de direcciones IP las cuales serán servidores de DNS, si hay más de uno realizarlo solo separadas por un espacio. Seleccionar ok.

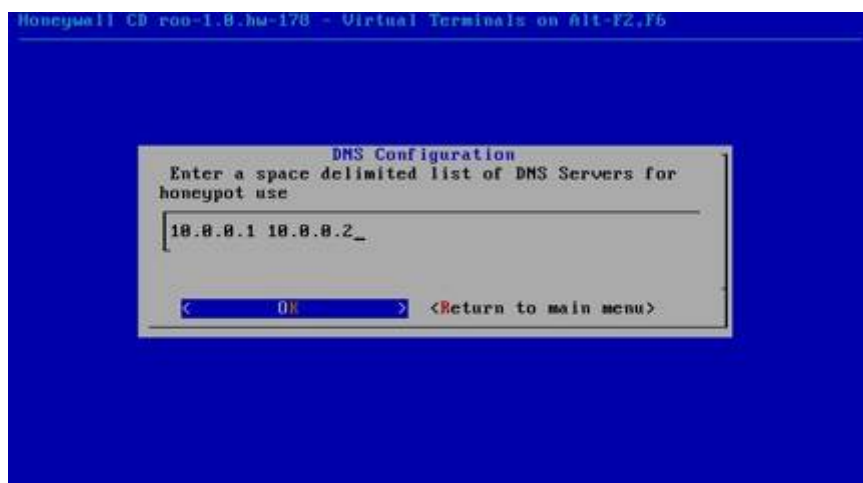


Figura 90. Configuración de IP de DNS.

Con la configuración de DNS se finalice la sección cuarta de configuración y se entra a la final en este aspecto la cual es sobre los mecanismos de alertas remotas. Seleccionar ok para proceder. Para este caso en particular no se configurará esta parte, con lo que se habrá terminado de la instalación del honeywall.



Figura 91. Mensaje de configuración final.

## Configuración de las variables de Sebek

Sebek es una herramienta de captura de datos diseñado para capturar las actividades de los atacantes en un honeypot. Tiene dos componentes, el primero es un cliente que se ejecuta en el honeypot y su objetivo es capturar todas las actividades de los atacantes (pulsaciones de teclado, envío de archivos, contraseñas) la cual la convierte y envía los datos al servidor. El segundo componente es el servidor que recopila los datos de los honeypots. El servidor normalmente se ejecuta en el Gateway Honeywall. Seleccionar “yes” para realizar las configuraciones de Sebek.

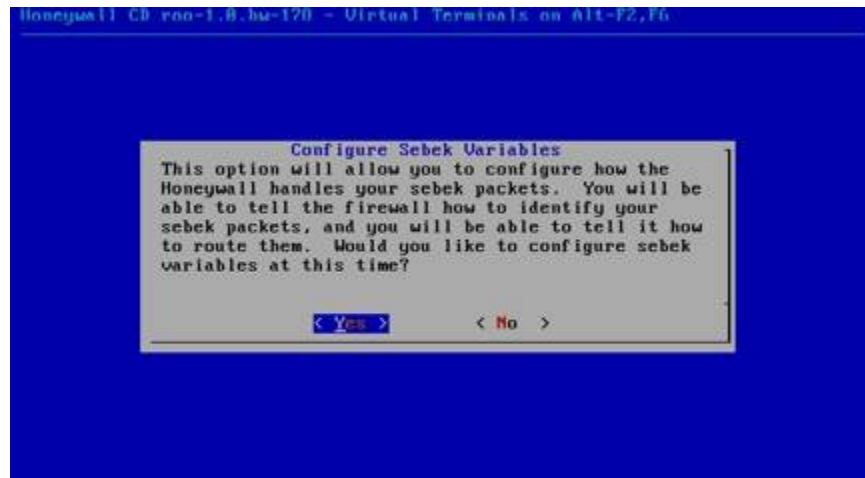


Figura 92. Configuración de las variables de Sebek.

Desde el honeywall se realiza la ejecución del servidor Sebek, el cual detectará automáticamente por medio de los paquetes Sebek. Escribir la dirección IP del Gateway (puerta de enlace) y seleccionar ok para proceder.



Figura 93. Configuración de las variables de Sebek.

Introducir el puerto UDP que utilizará Sebek y presionar intro en ok para proceder con la instalación. El valor que trae por defecto es el puerto 1101.



Figura 94. Configuración de las variables de Sebek.

Seleccionar la opción 4 “Accept and Log” y presionar intro en ok.



Figura 95. Configuración de las variables de Sebek.

Ingresa el nombre del honeywall y presionar intro en ok.

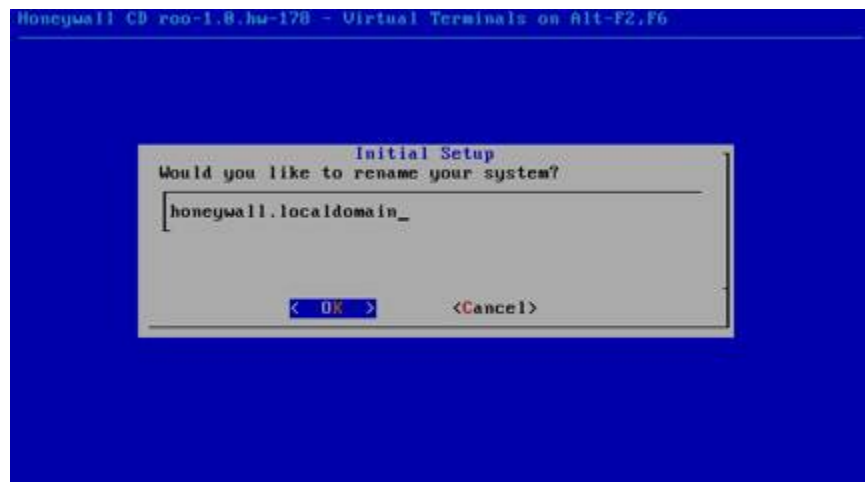


Figura 96. Configuración del nombre.

Como último paso aparecerá el mensaje "You have just finished the initial honeywall setup!.." lo cual significa que la configuración del honeywall ha llegado a su fin. Presionar intro en ok y esperar a que el sistema haga un reinicio.

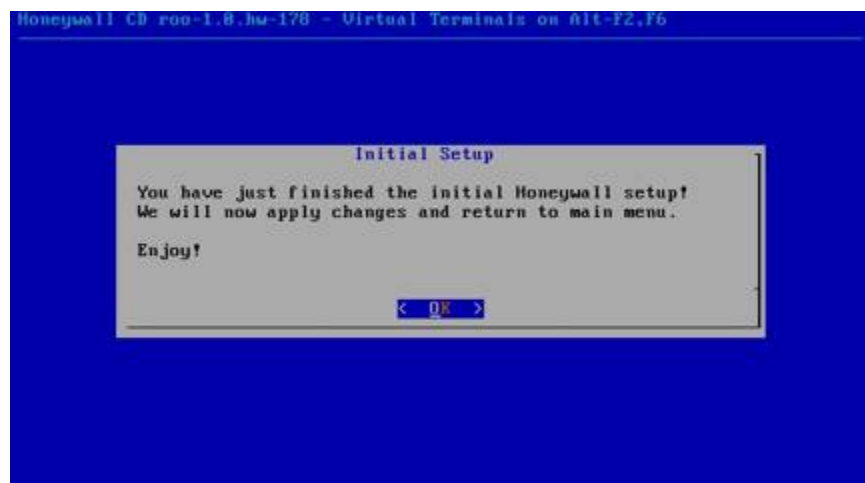


Figura 97. Mensaje de finalización de la configuración.

Después del reinicio se observará que el honeywall cargará varios servicios en línea de comando.

```
SIOCADDRT: File exists
Bringing up management interface: [ OK ]
Initializing MySQL database: [ OK ]
Starting MySQL: [ OK ]
Installing HFlow DB: [ OK ]
Stopping MySQL: [ OK ]
Starting MySQL: [ OK ]
Starting walleye-httpd: [ OK ]
Starting up Bridging mode: [ OK ]
Starting up Firewall: [ OK ]
Initializing inline mode
Starting Snort Inline: [ OK ]
Starting p0f: [ OK ]
Starting Argus: [ OK ]
Starting Snort: [ OK ]
```

Figura 98. Carga de archivos en línea de comando.

Una vez que los servicios han sido cargados el menú de configuración aparecerá, con el cual se puede realizar cambios a los valores ingresados anteriormente.



Figura 99. Menú de línea de comando.

## Mantenimiento de la aplicación del Honeywall

Después de que el honeywall está instalado se debe de mantener de forma adecuada. El nuevo Honeywall le da tres opciones para la configuración y el mantenimiento de la instalación.

Dialogo de Menú: es la clásica interfaz a la administración de los Honeywall, semejante a un entorno de selección en línea de comando. Este puede ser cargado en la línea de comando escribiendo menú. “# menu”

## Walleye

Es la interfaz basada en web para la administración del honeywall. El honeywall se ejecuta en un servidor web que puede ser conectado remotamente con más de una conexión SSL en la interfaz de administración. Esta interfaz gráfica permite al usuario configurar y mantener el sistema. Tiene un menú de la ampliación de lo que simplifica el acceso y la visualización de toda la información.

También viene con más profundidad en las explicaciones de las diferentes opciones. También cuenta con diferentes funciones, permitiendo a las organizaciones controlar quién puede acceder a través de la interfaz lo que dependiendo de la función que se les ha asignado. La principal ventaja de Walleye es el fácil uso. Para iniciarlo solamente se necesita ingresar en buscador de internet la dirección de administración que fue designada anteriormente, siendo la nomenclatura **https:// dirección de administración**. Lo cual desplegará como la siguiente figura. El usuario por defecto de configuración es roo y la contraseña honeywall. Luego de eso pedirá realizar el cambio de la contraseña.



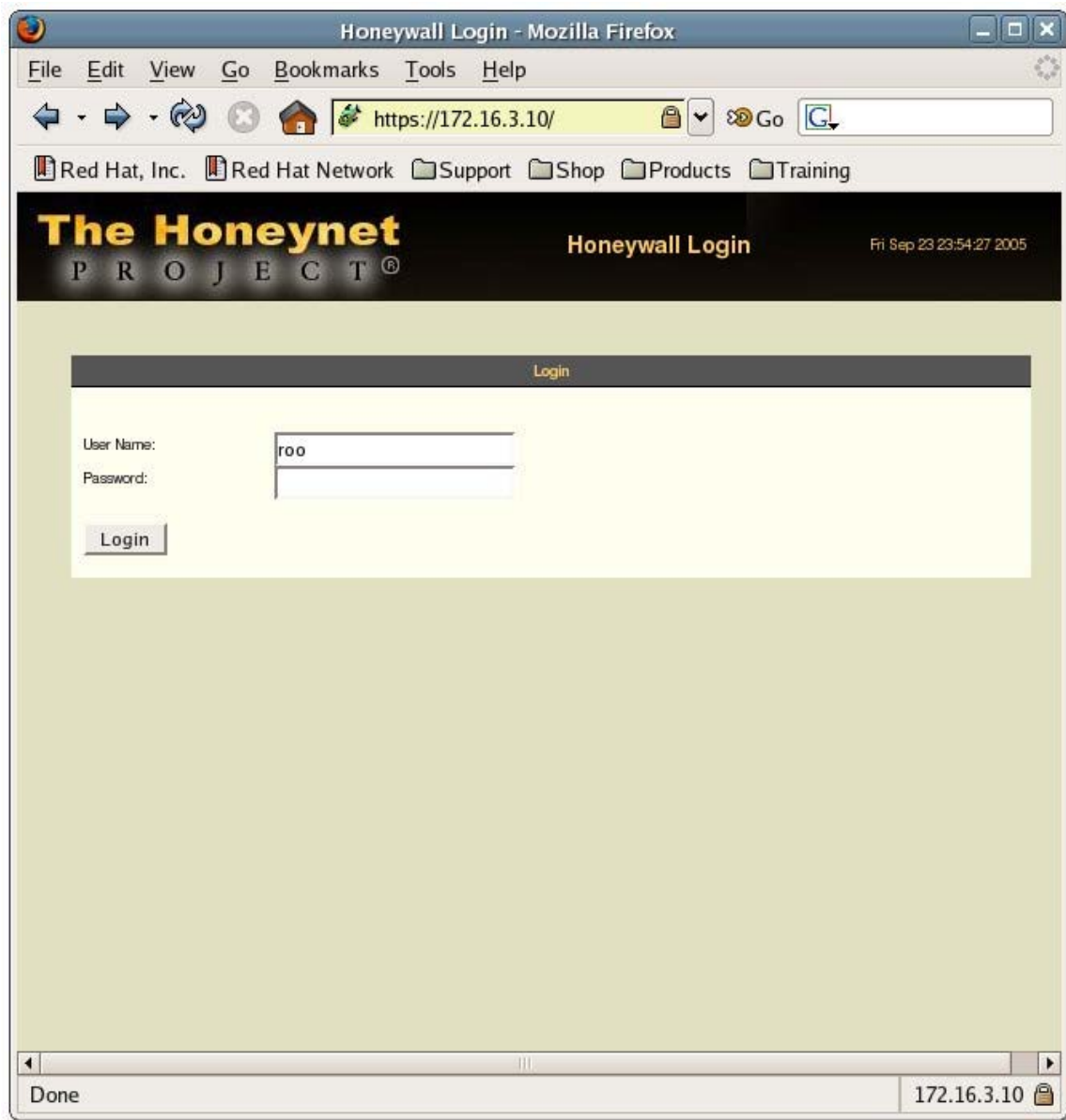


Figura 100. Pantalla de validación de walleye.

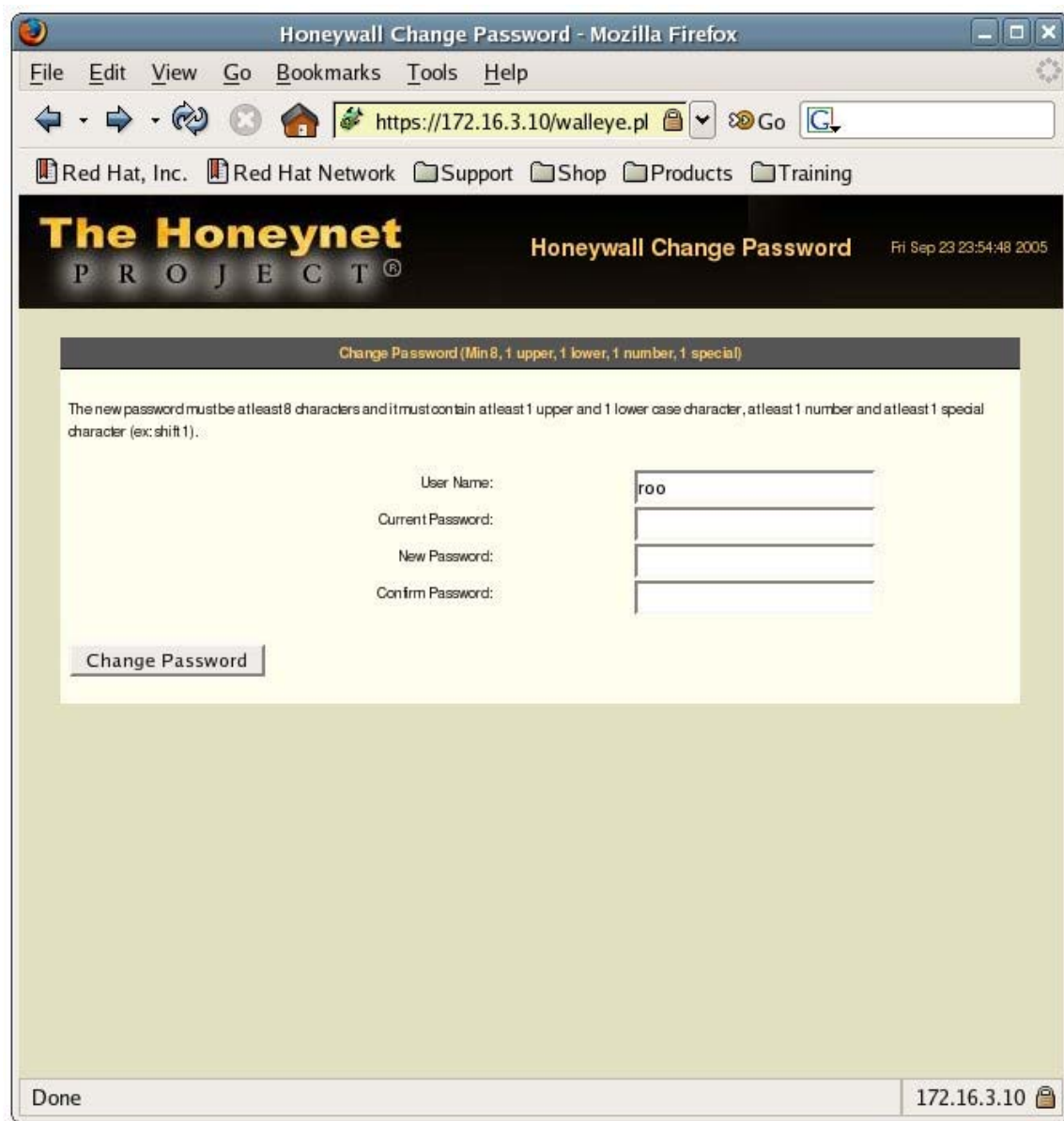


Figura 101. Pantalla de cambio de contraseña para validación de walleye.

La interfaz de análisis de datos “Data Analysis” se desplegará a continuación como se muestra en la siguiente figura.

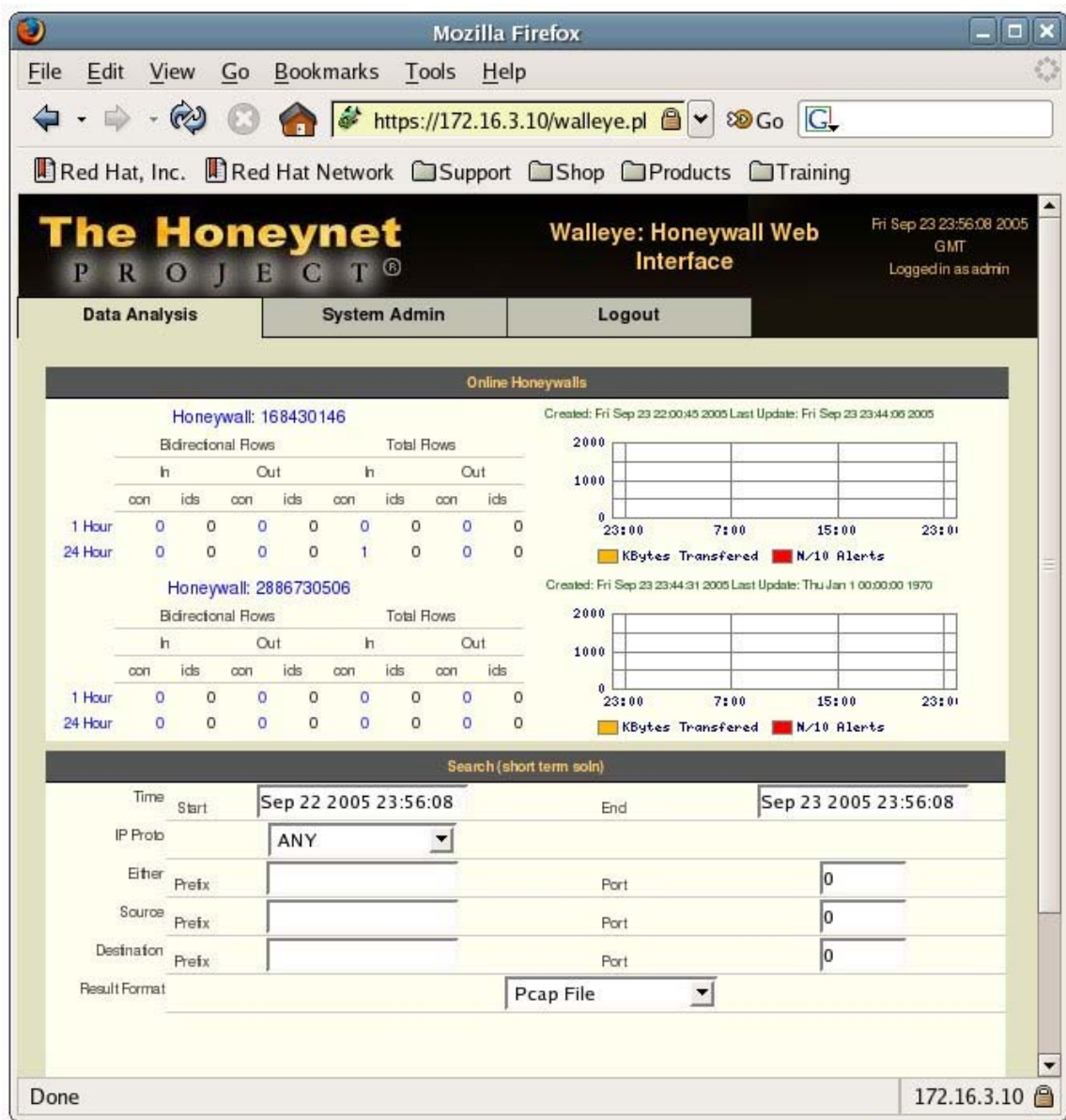


Figura 102. Pantalla de análisis de datos.

La interfaz de administración del sistema “System Admin” permitirá administrar el honeywall desde el web.

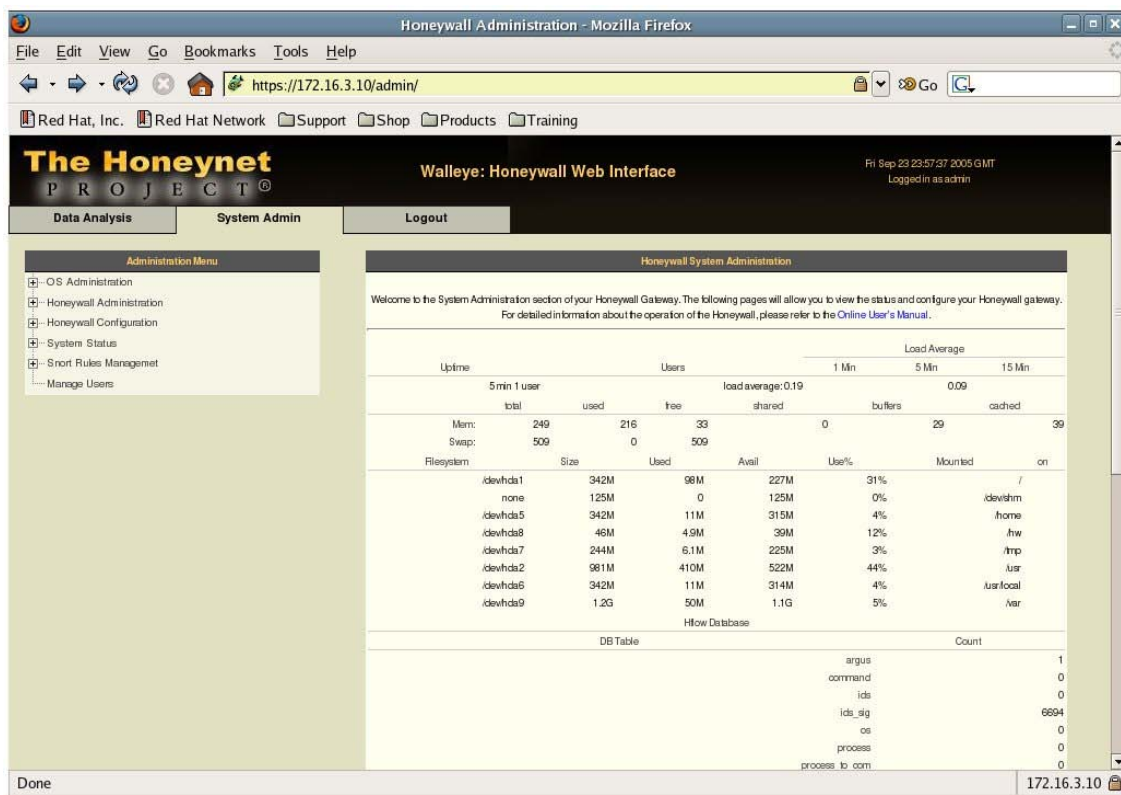


Figura 103. Pantalla de la administración del sistema.

Luego de esto, se podrá hacer la administración del honeywall, actualización de firmas y demás.

## Instalación y configuración de sistemas y herramientas de terceros

### SEBEK

Sebek es una herramienta que tiene el potencial de ser usado de forma involuntaria o maliciosa. Como es una buena herramienta para monitorizar intrusos, también puede ser útil para los intrusos usarla en sistemas comprometidos para recopilar contraseñas o espiar a los usuarios. Para reducir el potencial dañino de Sebek, se han tomado algunas decisiones.

En las primeras versiones de Sebek, los datos exportados se encriptan y las cabeceras de los paquetes se suplantaban para ocultar el origen de los datos. El actual método de ocultación sólo funciona con sistemas trampa que tengan Sebek instalado, cualquier otro sistema en la LAN puede ver los paquetes de Sebek en texto claro.

Esto supone que si un intruso intenta utilizar Sebek en sus propios sistemas comprometidos, las organizaciones lo detectarán fácilmente porque podrán ver los datos de Sebek exportados a la red. Para reducir más las posibilidades de abuso se han eliminado las características estándar de rootkit que poseía Sebek. Así que un intruso no tendría un único LKM habilitando la captura de contraseñas y características de rootkit

## **Instalación del cliente SEBEK**

La instalación del cliente implica compilarlo para la versión del núcleo que se tendrá en nuestro sistema trampa honeynet. Una vez que el cliente se ha compilado correctamente, se tendrá un archivo *tar* preparado para copiarlo al sistema trampa o del honeynet. Este archivo *tar* incluye el fichero *sbk\_install.sh*.

Este fichero contiene tanto los comandos para instalar Sebek como las variables de configuración. Para instalar Sebek, simplemente se deberá de editar las opciones que desee y ejecutar el guión de instalación en el sistema.

Al ejecutar *sbk\_install.sh* se instala el módulo para el núcleo con la configuración especificada. Hay seis valores configurables en el guión de instalación, y a menudo serán los mismos para todos los sistemas trampa.

### **IP Destino:**

Este campo define la dirección IP de destino usada para todos los paquetes Sebek generados. Como el servidor Sebek no tiene en cuenta la dirección IP destino cuando recolecta paquetes, no es necesario usar aquí la dirección del servidor. Además no es recomendable, ya que si por algún motivo el intruso pudiera ver los

paquetes podría identificar el sistema que muy probablemente esté realizando el control de datos en la red trampa.

#### **MAC Destino:**

Especifica la dirección MAC de destino para todos los paquetes. Como Sebek no usa ARP, esta es una opción obligatoria. Si el servidor está a más de un salto del sistema trampa entonces la dirección MAC de destino debe asignarse a la puerta de enlace (gateway) por defecto. Por último, usando el valor FF:FF:FF:FF:FF:FF causaremos que los paquetes sean distribuidos (esta es la dirección de broadcast) a cada máquina en la red LAN.

#### **Valor Mágico:**

Este valor se usa para identificar qué paquetes se deben ocultar del sistema trampa o del honeynet. Cuando se usa, Sebek no sólo utiliza este valor en la cabecera Sebek, sino que oculta los paquetes con este valor establecido. Es altamente recomendable que todas las instancias de Sebek en una LAN se configuren con el mismo Valor Mágico.

#### **Puerto Destino UDP:**

Define el puerto de destino UDP al que irán dirigidos los paquetes. Este valor es usado por el servidor para identificar los paquetes que le interesan.

#### **Sólo pulsaciones de teclas:**

Esta variable acepta dos valores: 1 ó 0. Si se activa, Sebek sólo recolectará pulsaciones de teclas. De otra forma Sebek recolecta todos los datos leídos. Esta variable no debe activarse si se quieren recuperar transferencias SCP.

**Pruebas:**

Esta opción es un indicador binario. Si el indicador está activo ocurren dos cosas, primero, el módulo del núcleo no se oculta y segundo, se activa una depuración adicional en el módulo. Es de tener mucho cuidado porque esta depuración adicional puede delatar la presencia de Sebek, ya que envía datos de depuración a través de Syslog.

Cuando se están configurando sistemas trampa en la misma red LAN es importante que todos usen el mismo valor mágico. Esto impedirá que un sistema trampa pueda ver los paquetes de otro. Cuando se configuren las direcciones IP y MAC, es de tener en cuenta que el valor de la MAC es el más importante. Si se especifica incorrectamente la dirección IP destino pero configura la MAC correctamente, los registros de Sebek llegarán al servidor, suponiendo que el puerto UDP es correcto.

Además, cuando el servidor se está ejecutando en un Honeywall Gateway, la interfaz no tiene IP configurada asignada, así que la única forma de asegurarse que los paquetes son registrados por el servidor es configurar la dirección MAC de destino con la puerta de enlace por defecto o la dirección MAC del Honeywall.

Si va a registrar datos de forma remota (a una máquina que no está en la LAN), entonces la dirección IP debe asignarse a la IP de dicha máquina, y la dirección MAC debe asignarse a la dirección de la puerta de enlace de la red LAN. Después de la configuración, la ejecución de `sbk_install.sh` instalará el cliente de Sebek, y empezará a capturar y exportar datos.

**Instalación del Servidor**

El servidor tiene dos posibles fuentes para recuperar datos del cliente de Sebek. La primera opción es obtener los datos de la red desde un registro estándar de `tcpdump`, y extraer sólo los datos de Sebek de dicho registro.

La segunda opción es capturar directamente el tráfico en la red. La extracción de datos desde un fichero tcpdump proporciona la capacidad de examinar datos archivados o datos a los que no se ha tenido acceso directo.

El servidor está compuesto de hasta tres componentes. El primero se llama sbk\_extract. Este puede capturar datos directamente desde un interfaz actuando como un rastreador, o recogerlos de un fichero tcpdump. De cualquier forma debe usar esta herramienta para recuperar los datos de Sebek. Una vez que sbk\_extract extrae los datos, puede hacer dos cosas con ellos. La primera opción es enviarlos a una herramienta llamada sbk\_ks\_log.pl, que es un programa en Perl que recoge las pulsaciones de teclas del intruso y las envía a la salida estándar.

La segunda opción es usar sbk\_upload.pl, que es otro programa en Perl que almacena los datos de Sebek en una base de datos mysql. Para compartir o archivar los datos, es recomendable que se trabaje con las capturas binarias de tcpdump como fuente canónica de datos. Como es común el hecho de registrar todo el tráfico que entra y sale de una red trampa, este archivado ya se realiza y la aparición del archivado para Sebek no supone un esfuerzo adicional.

sbk\_extract es la aplicación que extrae los registros de Sebek de los datos de entrada. Independientemente del tipo de análisis, esta es la primera aplicación en la cadena. Esta aplicación recoge los paquetes de Sebek de la red o de un fichero, y entonces envía los registros encontrados a la utilidad especificada. Tenemos tres parámetros:

- f Especifica el fichero del que extraer los datos.
- i Define la interfaz en la que capturar datos.
- p Especifica el puerto UDP destino elegido en el cliente.



**Guardar los registros de Sebek en una base de datos:**

Ejecutar sbk\_extract y redirigir la salida a sbk\_upload.pl.

ejemplo: sbk\_extract | sbk\_upload.pl.

**Monitorización desde la línea de comandos:**

Ejecutar sbk\_extract y redirigir la salida a sbk\_ks\_log.pl.

ejemplo: sbk\_extract | sbk\_ks\_log.pl

**Análisis personalizado:**

Ejecutar sbk\_extract y redirigir la salida a su aplicación de monitorización personalizada.

**Monitorización desde la línea de comandos**

sbk\_ks\_log.pl le permite visualizar la actividad de pulsaciones de teclas en la máquina donde ha instalado el cliente de Sebek desde la línea de comandos del servidor. No necesita parámetros de ejecución y toma su entrada de sbk\_extract a través de la entrada estándar. Ejemplo de esto es: sbk\_extract -i eth0 -p 1101 | sbk\_ks\_log.pl

En este ejemplo, sbk\_Extract está capturando datos en la interfaz eth0 y esperando los registros en el puerto UDP 1101. Entonces envía estos registros a sbk\_ks\_log.pl para la extracción de las pulsaciones de teclas. Un ejemplo de la salida de sbk\_ks\_log.pl puede verse a continuación en la siguiente figura 104

```
[2003-07-23 20:03:45 10.0.0.13 6673 bash 500]whoami
[2003-07-23 20:03:48 10.0.0.13 6673 bash 500]who
[2003-07-23 20:03:50 10.0.0.13 6673 bash 500]su
[2003-07-23 20:03:57 10.0.0.13 6886 bash 0]cd /var/log
[2003-07-23 20:03:57 10.0.0.13 6886 bash 0]ls
[2003-07-23 20:04:01 10.0.0.13 6886 bash 0]mkdir ...
[2003-07-23 20:04:20 10.0.0.13 6886 bash 0]tcsh
[2003-07-23 20:04:20 10.0.0.13 6921 tcsh 0]0
[2003-07-23 20:04:20 10.0.0.13 6920 tcsh 0]vt
[2003-07-23 20:04:20 10.0.0.13 6920 tcsh 0]en
[2003-07-23 20:04:20 10.0.0.13 6920 tcsh 0]en
[2003-07-23 20:04:27 10.0.0.13 6920 tcsh 0]cd /tmp
[2003-07-23 20:04:28 10.0.0.13 6920 tcsh 0]ls
[2003-07-23 20:04:42 10.0.0.13 6920 tcsh 0]cd /usr/lib
[2003-07-23 20:04:42 10.0.0.13 6920 tcsh 0]ls
```

Figura 104. Salida de información sebek.

La salida de sbk\_ks\_log.pl es similar a lo que un usuario ve en su terminal. Sin embargo, sólo vemos los comandos introducidos y no la salida de dichos comandos. Los caracteres de control son escapados cuando aparecen. Por ejemplo, cuando pulsamos la tecla de borrado, se reemplaza con la cadena [BS]. Cada línea visualizada tiene el siguiente formato:

[Marca\_de\_tiempo Dir\_IP PID Comando UID] Texto

- Marca\_de\_tiempo. Tiempo en que se introdujo la primera pulsación del comando.
- Dir\_IP. Dirección de la máquina trampa.
- PID. Identificador del proceso.
- Comando. Primeros 10 caracteres del comando.
- UID. ID de usuario propietario del proceso.

## Guardando Datos de Sebek en una Base de Datos

sbk\_upload.pl es el programa que se encarga de guardar los registros en una base de datos *mysql*. Hay algunas opciones disponibles para este programa:

- u Usuario de la base de datos
- s Servidor de la base de datos, por defecto es la máquina local.
- d Nombre de la base de datos.
- p Contraseña.
- P Puerto donde escucha la BD.

Ejemplo:

```
sbk_extract -i eth0 -p 1101 | sbk_upload.pl -u Sebek -p secret -d Sebek
```

Al igual que en el ejemplo anterior, busca paquetes destinados al puerto UDP 1101 y está capturando datos en la interfaz eth0. Los registros extraídos se envían a sbk\_upload.pl, que los guarda en una base de datos de la máquina local usando el usuario "Sebek", la contraseña "secret" y lo inserta en la base de datos llamada "Sebek". Se inserta cada registro en la base de datos *mysql*.

Una vez que los registros se han insertado en la base de datos, pueden ser visualizados usando la interfaz Web o accedida directamente a través de consultas SQL.

## El interfaz Web

Ahora Sebek viene acompañado de un interfaz de análisis vía Web. Este interfaz proporciona a los usuarios la capacidad de monitorizar la actividad de pulsaciones de teclas, buscar una actividad específica, recuperar ficheros copiados con SCP y en general proporciona una mejor capacidad de acceder a los datos. La interfaz está implementada con PHP y sólo examina los datos introducidos en la base de datos; no usa datos de otras fuentes como capturas de paquetes o mensajes *syslog*.

Está diseñado para soportar el trabajo que implica una investigación forense, sin embargo requiere unos conocimientos técnicos mínimos para entenderlo. La intención fue hacer esta herramienta para Sebek como Ethereal lo es para las capturas de datos. La interfaz tiene tres opciones primarias: ver las pulsaciones de teclas, búsquedas y navegación.

- El resumen de pulsaciones proporciona un resumen de la actividad de pulsaciones de teclas.
- La búsqueda permite a los usuarios buscar información concreta.
- La navegación, proporciona un resumen de todas las actividades, incluyendo otras diferentes de las pulsaciones de teclas.

En las figuras siguientes, un usuario entra a una máquina trampa con dirección IP 10.0.1.13. Después de entrar, el usuario descarga un fichero llamado “malware”. Este fichero es un ejecutable binario protegido con Burneye. “malware” es una herramienta utilizada para conseguir acceso no autorizado como root. El usuario ejecuta “malware” y consigue acceso como root a la máquina trampa. El intruso sólo habrá conseguido acceso a una máquina trampa.

Sebek se había configurado en el cliente para registrar todos los datos y enviarlos a la dirección MAC de la pasarela Honeywall. En el Honeywall, se estará ejecutando sbk\_extract redirigiendo la salida a sbk\_upload.pl. El resto de máquinas trampa en la red LAN también pueden tener Sebek instalado. Para evitar que el tráfico de Sebek sea detectado por un intruso o atacante, todas las máquinas trampa usarán el mismo Valor Mágico. En el ejemplo se demostrará la capacidad de la interfaz para:

1. Recuperar un fichero copiado mediante SCP.
2. Identificar la contraseña usada para habilitar el binario Burneye.
3. Identificar el punto exacto donde el intruso consiguió acceso como root.



Figura 105. Vista general del sistema

La vista general del sistema, proporciona una lista de todos los sistemas que estamos monitorizando y la última vez en que se observa actividad en dicho sistema. Dando clic en el botón de pulsaciones de teclas podemos obtener un resumen de la actividad en el sistema.

Sebek

Home | Keystrokes | Browse | Search

Sun, 27 Jul 2003 15:46:40 -0500

Keystroke Summary View for IP: 10.0.1.13

Details	IP	PID	UID	COMMAND	FD	DATA
	10.0.1.13	1318	0	sh	0	[2003-07-23 20:04:33]# ls [2003-07-23 20:04:34]# less messages [2003-07-23 20:04:52]# cd /etc [2003-07-23 20:04:54]# mkdir ... [2003-07-23 20:04:57]# ls
	10.0.1.13	1323	0	less	3	[2003-07-23 20:04:35]# \000 [2003-07-23 20:04:50]# q
	10.0.1.13	1321	0	w	6	[2003-07-23 20:04:09]# w\000
	10.0.1.13	1271	500	bash	0	[2003-07-23 20:03:29]# ho[BS] [BS] who [2003-07-23 20:03:33]# w [2003-07-23 20:03:43]# ./malware [2003-07-23 20:03:47]# chmod ux[BS] +x mal [2003-07-23 20:03:52]# ./mal
	10.0.1.13	1312	500	w	6	[2003-07-23 20:03:33]# w\000
	10.0.1.13	1271	500	bash	3	[2003-07-23 20:03:24]# [BS] [BS]
	10.0.1.13	1304	500	tput	3	[2003-07-23 20:03:24]# \000
	10.0.1.13	1305	500	wc	0	[2003-07-23 20:03:24]# [BS]
	10.0.1.13	1307	500	tput	3	[2003-07-23 20:03:24]# \000
	10.0.1.13	1302	500	tput	3	[2003-07-23 20:03:24]# \000
	10.0.1.13	1252	0	mingetty	0	[2003-07-23 20:03:16]# b!ackhat
	10.0.1.13	1263	0	sshd	7	[2003-07-23 20:02:07]# \000\000\000
	10.0.1.13	1264	500	scp	0	[2003-07-23 20:02:07]# C0664 38802 malware [2003-07-23 20:02:09]# \000
	10.0.1.13	1263	0	sshd	3	[2003-07-23 20:02:09]# \000
		0		sshd	4	[2003-07-23 20:02:02]# SSH-2.0-OpenSSH_3.1p1

Document: Done (0.127 secs)

de reducir la cantidad de datos sin interés es usar el interfaz de búsqueda para buscar actividad por el nombre del intérprete de comandos utilizado. El siguiente paso será entrar en detalle con el PID 1264 para observar y recuperar una copia de “malware”.

The screenshot shows the Sebek web interface in a Mozilla browser window. The page title is "Sebek" and the date is "Sun, 27 Jul 2003 15:46:52 -0500". The main content area is titled "Details" and shows information for PID 1264. The IP is 10.0.1.13, the command is "scp bash sshd", and the UID is 500 0. Below this is a table of system reads and a section for SCP file transfer details.

View as:			sys_read Data Context					
SCP File Transfer	Text / Keystrokes	Raw Data	UID	File Desc	Command	Start	End	Total Bytes
			500	0	scp	2003-07-23 20:02:07	2003-07-23 20:02:09	38823 bytes read
			500	3	bash	2003-07-23 20:02:07	2003-07-23 20:02:07	5249 bytes read
			500	3	scp	2003-07-23 20:02:07	2003-07-23 20:02:07	10172 bytes read
			0	7	sshd	2003-07-23 20:02:07	2003-07-23 20:02:07	3383 bytes read

**SCP File Transfer Decode for PID 1264 FD 0**

File Name: [malware](#)  
Expected Size: 38802 bytes  
Observed Size: 38802 bytes  
Permissions: C0664  
Lost 0 bytes

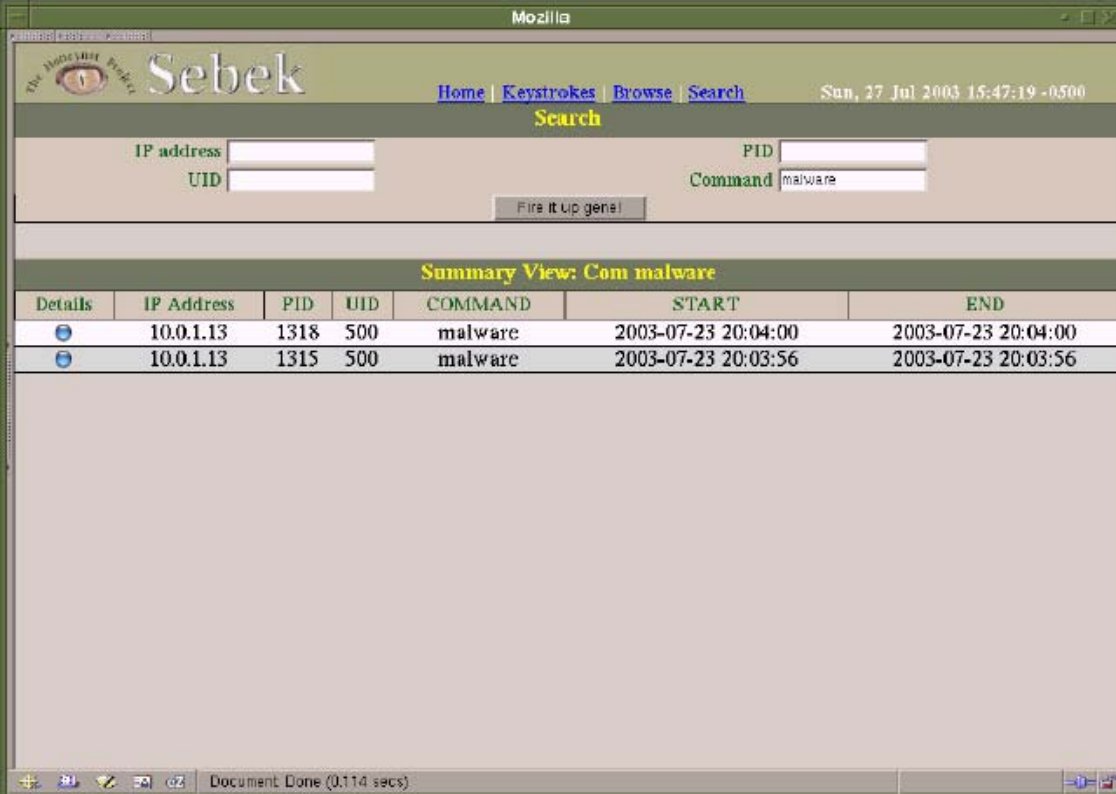
Figura 107. Detalles para el PID 1264.

La vista de detalles de la figura anterior, muestra toda la actividad para un determinado PID. En este caso estamos trabajando con el PID 1264. Lo que vemos es una transferencia SCP de entrada al sistema trampa. Se puede observar que la interfaz ha detectado que el Descriptor de Fichero 0 corresponde a los contenidos de la transferencia, y lo representa proporcionando un botón SCP.

Accediendo a dicho botón, la parte inferior de la vista ofrece los datos del FD0 como un fichero. Como Sebek usa el puerto UDP para exportar los datos hay posibilidades de que se pierdan datos; especialmente en transferencias entre

redes LANs. Para advertir de esta diferencia, la interfaz ofrece los tamaños esperados y observados del fichero. Accediendo al nombre del fichero podemos descargarlo. Si descarga y ejecuta el string sobre el binario podrá ver que está protegido con Burneye. La utilidad strings es útil para extraer datos en texto claro de los ficheros binarios.

En el caso de los binarios ELF protegidos con Burneye, una de las primeras cadenas en el binario nos permite identificar positivamente la existencia de Burneye. Ahora que se ha recuperado el fichero e identificado como un binario Burneye, se recuperará la contraseña utilizada para activar el binario.



Summary View: Com malware						
Details	IP Address	PID	UID	COMMAND	START	END
	10.0.1.13	1318	500	malware	2003-07-23 20:04:00	2003-07-23 20:04:00
	10.0.1.13	1315	500	malware	2003-07-23 20:03:56	2003-07-23 20:03:56

Figura 108. Resultados de la búsqueda para el comando “malware”.



Se observará que dos procesos con PID 1315 y 1518, se ejecuta el comando “malware”. El siguiente paso será examinar el PID 1315 en detalle ya que este proceso terminó primero. Para examinarlo, simplemente pulsamos el correspondiente botón de Detalles.



Cuando se entra en los detalles del PID 1318 de la figura anterior, sólo se observa un FD activo. Pulsando en Texto/Pulsaciones, se verá la actividad del FD 3. La primera línea parece ser texto llano; la segunda parece un binario ELF. La primera línea es interesante. Son los primeros datos leídos por cualquier instancia de “malware” y del análisis anterior sabemos que “malware” es un binario Burneye. Para que un binario Burneye se ejecute, lo primero que debe ocurrir es que se debe activar mediante una contraseña.

Aunque la interfaz no muestra esto explícitamente, esta primera línea es la contraseña utilizada para activar el binario. Llegados a este punto, se ha demostrado como recuperar un fichero copiado mediante SCP, y como recuperar la contraseña de un binario protegido con Burneye. La última tarea será identificar en qué momento el intruso consiguió acceso como root. Para conseguirlo se examinará la otra instancia de “malware”.



Figura 110. Detalles para el PID 1318

El PID 1318 corresponde a la otra instancia de “malware” y ofrece mucha información. El proceso empieza a ejecutarse con el nombre de “malware” y acaba con el de “sh”. Más importante, empieza su ejecución con un UID 500 y acaba con UID 0, o root. Así sabemos que usando este PID el usuario consiguió acceso como root. El usuario consiguió este acceso en la fecha 23-07-2003 20:04:01 GMT.

## **Configuración de SNORT**

Para realizar la configuración, es necesario realizar la autenticación como usuario root mediante la orden “su -”, con lo que se posicionará en el directorio donde se ha descargado todos los archivos anteriores. Seguidamente se realizará la siguiente secuencia en la línea de comandos para la configuración del snort, es de hacer notar que el punto en cada final de línea es para propósitos de separación y diferenciación de línea en el documento pero no debe de ser puesto en la línea de comando:

```
tar -xvzf zlib-1.1.4.tar.gz.
```

```
cd zlib-1.1.4.
```

```
./configure; make test.
```

```
make install.
```

```
cd ..
```

```
tar -xvzf libpcap-0.8.1.tar.gz.
```

```
cd libpcap-0.8.1.
```

```
./configure.
```

```
Make.
```

```
make install.
```

```
cd ..
```

```
groupadd mysql.
```

```
useradd -g mysql mysql.
```

Luego se debe de configurar el archivo `/root/.bash_profile` para que el `PATH` sea `PATH=$PATH:$HOME/bin:/usr/local/mysql/bin`.

```
tar -xvzf mysql-4.0.16.tar.gz.  
cd mysql-4.0.16.  
./configure --prefix=/usr/local/mysql.  
Make.  
make install.
```

```
scripts/mysql_install_db.  
chown -R root /usr/local/mysql.  
chown -R mysql /usr/local/mysql/var.  
chgrp -R mysql /usr/local/mysql.  
cp support-files/my-medium.cnf /etc/my.cnf.  
echo /usr/local/mysql/lib/mysql >> /etc/ld.so.conf.  
echo /usr/local/lib >> /etc/ld.so.conf.
```

Antes de proceder se deberá de probar la funcionalidad de la base de datos para observar que no existan errores. Se ejecutará de la siguiente forma:

ejecutar `/usr/local/mysql/bin/mysqld_safe --user=mysql &`.

```
cp support-files/mysql.server /etc/init.d/mysql.  
cd /etc/rc3.d.  
ln -s ../init.d/mysql S85mysql.  
ln -s ../init.d/mysql K85mysql.  
cd /etc/rc5.d.  
ln -s ../init.d/mysql S85mysql.  
ln -s ../init.d/mysql K85mysql.  
cd ../init.d.  
chmod 755 mysql.
```

cd <en el directorio de paquetes descargados>.

tar -xvzf httpd-2.0.48.tar.gz.

cd httpd\_2.0.48.

./configure --prefix=/www --enable-so.

Make.

make install.

cd ..

tar -xvzf php-4.3.4.tar.gz.

cd php-4.3.4.

./configure --prefix=/www/php --with-apxs2=/www/bin/apxs --with-config-filepath=/www/php --enable-sockets --with-mysql=/usr/local/mysql --with-zlibdir=/usr/local --with-gd (todo esto deberá de estar en una línea)

make.

make install.

cp php.ini-dist /www/php/php.ini.

echo LoadModule php4\_module modules/libphp4.so >>/www/conf/httpd.conf

echo AddType application/x-httpd-php.php.

cd /www/bin.

cp apachectl /etc/init.d/httpd.

cd /etc/rc3.d.

ln -s ../init.d/httpd S85httpd.

ln -s ../init.d/httpd K85httpd.

cd /etc/rc5.d.

ln -s ../init.d/httpd S85httpd.

ln -s ../init.d/httpd K85httpd.

/etc/rc5.d/S85httpd start.

cd <directorio de archivos descargados>.

```
mkdir /etc/snort.  
mkdir /var/log/snort.  
tar -xvzf snort-2.1.0.tar.gz.  
cd snort-2.1.0.  
./configure --with-mysql=/usr/local/mysql.  
Make.  
make install.
```

```
cd /etc/snort/rules.  
cp * /etc/snort.  
cd ../etc.  
cp snort.conf /etc/snort.  
cp *.config /etc/snort.
```

Luego de esto se procederá a modificar el archivo snort.conf:

Configuración de la red a monitorizar: var HOME\_NET 10.1.1.0/24.  
Configurar el directorio donde están los archivos de reglas: var RULE\_PATH /  
etc/snort/.

Configuración de la base de datos (en una línea): output database: log, mysql,  
user=snort password=la\_contraseña dbname=snort host=localhost  
75)cp /etc/snort/contrib/S99snort /etc/init.d/snort.

Cambiar en el archivo /etc/init.d/snort las siguientes lineas:

```
CONFIG=/etc/snort/snort.conf.  
#SNORT_GID=nogroup --> hacer que esta linea sea un comentario.  
$SNORT_PATH/snort -c $CONFIG -i $IFACE $OPTIONS --> remover -g  
$SNORT_GID.  
cd /etc/init.d.
```

```
chmod 755 snort.  
cd /etc/rc3.d.  
ln -s ../init.d/snort S99snort.  
ln -s ../init.d/snort K99snort.  
cd /etc/rc5.d.  
ln -s ../init.d/snort S99snort.  
ln -s ../init.d/snort K99snort.  
/usr/local/mysql/bin/mysql.
```

```
mysql> SET PASSWORD FOR root@localhost=PASSWORD('mi_contraseña');  
mysql> create database snort;.  
mysql> grant INSERT,SELECT on root.* to snort@localhost;.  
mysql> exit.  
cd /<directorio de archivos descargados>/snort-2.1.0.  
/usr/local/mysql/bin/mysql -p <./contrib/create_mysql snort.  
>Enter password: my_contraseña.  
cd contrib.  
zcat snortdb-extra.gz |/usr/local/mysql/bin/mysql -p snort.  
cd <directorio de archivos descargados>.  
cp jpgraph-1.14.tar.gz /www/htdocs.  
cd /www/htdocs.  
tar -xvzf jpgraph-1.14.tar.gz.  
rm -rf jpgraph-1.14.tar.gz.  
cd jpgraph-1.14.  
rm -rf README.  
rm -rf QPL.txt.  
cd <directorio de archivos descargados>.  
cp adodb330.tgz /www/htdocs.  
cd /www/htdocs.  
tar -xvzf adodb330.tgz.  
rm -rf adodb330.tgz.
```

```
cd <directorio de archivos descargados>.
```

```
cp base-0.9.6b23.tar.gz /www/htdocs.
```

```
cd /www/htdocs.
```

```
tar -xvzf base-0.9.6b23.tar.gz.
```

```
rm -rf base-0.9.6b23.tar.gz.
```

```
cd base.
```

```
vi base_conf.php .
```

Despues de esta sentencia se deben de realizar los siguientes cambios:

```
$DBlib_path = "/www/htdocs/adodb";.
```

```
$DBtype = "mysql";.
```

```
$alert_dbname = "snort";.
```

```
$alert_host = "localhost";.
```

```
$alert_port = "";
```

```
$alert_user = "root";.
```

```
$alert_password = "mi_contraseña";.
```

```
$archive_dbname = "snort";.
```

```
$archive_host = "localhost";.
```

```
$archive_port = "";
```

```
$archive_user = "root";.
```

```
$archive_password = "mi_contraseña";.
```

```
$ChartLib_path = "/www/htdocs/jpgraph-1.11/src";.
```

```
$chart_file_format="png";.
```

## **Configuración de BASE**

Base es la interfaz en PHP que con la cual se relacionará para ver las alertas, eliminarlas, clasificarlas, etc. La carga para la instalación se deberá de hacer de la siguiente forma:



```
# cd /var/www/htdocs
# wget http://belnet.dl.sourceforge.net/sourceforge/secureideas/base-1.2.6.tar.gz
# tar zxvf base-1.2.6.tar.gz
# mv base-1.2.6 base
# rm base-1.2.6.tar.gz
```

Una vez descargado se realizará la configuración, esta se centrará en el fichero `base_conf.php` que se debe copiar de la plantilla que se proporciona:

```
# cp /var/www/htdocs/base/base_conf.php.dist
/var/www/htdocs/base/base_conf.php
```

Despues de realizado esto se procederá a la configuración del fichero `base_conf.php`.

```
linea 44: $BASE_urlpath= '/base';
linea 66: $DBlib_path = '/var/www/htdocs/base/adodb/';
linea 87: $alert_dbname = 'snort';
linea 90: $alert_user = 'root';
linea 91: $alert_password = 'tu_contraseña_BBDD';
```

Se deberá de guardar el fichero y se debe de salir. El siguiente paso a realizar es copiar las firmas del Snort al directorio de BASE, estas firmas son ficheros en texto plano con detalles sobre las alertas del Snort, que servirán como información para leer cuando salten dichas alertas, se deberpa de copiar a su destino adecuado con los siguientes comandos:

```
# mkdir /var/www/htdocs/base/signatures
# cp /usr/lib/snort-2.6.0.1/signatures /var/www/htdocs/base/signatures
```

Luego que se tiene BASE configurado, ahora se deberá de poner un método de autenticación, para que el acceso a BASE esté restringido a un usuario con

contraseña. Para ello se creará el fichero `/var/www/htdocs/base/.htaccess` y se le debe de poner el siguiente contenido:

```
AuthName ?Base Access?
```

```
AuthType Basic
```

```
AuthUserFile /var/www/htdocs/base/htpasswd.users
```

```
require valid-user
```

## **Instalación de ADODB**

ADODB será un intermediario entre BASE y MySQL, su instalación es muy sencilla e independiente de la distribución de Linux que se utilice, basta con escribir los siguientes comandos:

```
cd /var/www/htdocs/base
```

```
wget http://ovh.dl.sourceforge.net/sourceforge/adodb/adodb491.tgz
```

```
tar zxvf adodb491.tgz
```

```
rm adodb491.tgz
```

## **Instalación de los módulos PEAR**

PEAR es un FrameWork de PHP el cual se instala junto con PHP5, a través de él se instalará unos módulos de los que se servirá BASE para crear los gráficos de las alertas. Los comandos son los siguientes:

```
# cd /var/www/htdocs/base
```

```
# wget http://pear.php.net/get/Image_Color-1.0.2.tgz
```

```
# tar zxvf Image_Color-1.0.2.tgz
```

```
# rm Image_Color-1.0.2.tgz
```

```
# pear install Image_Color-1.0.2.tgz
```

```
# wget http://pear.php.net/get/Image_Canvas-0.3.0.tgz
```

```
# tar zxvf Image_Canvas-0.3.0.tgz
```

```
# rm Image_Canvas-0.3.0.tgz
```

```
# pear install Image_Canvas-0.3.0.tgz

# wget http://pear.php.net/get/Image_Graph-0.7.tgz
# tar zxvf Image_Graph-0.7.2.tgz
# rm Image_Graph-0.7.2.tgz
# pear install Image_Graph-0.7.2.tgz
```

## Configuración web de BASE

Ahora se terminará de configurar de forma web el BASE, para ello se ejecutará en el navegador dirección configurada de la siguiente forma, el local host es la dirección IP en donde reside el sistema snort:

[http://localhost/base/base\\_main.php](http://localhost/base/base_main.php)

Con este paso se observará una ventana como la de la figura siguiente. En ella se recibirá un mensaje de alerta indicando que la BBDD de Snort está incompleta ya que le falta la estructura adicional para que BASE funcione correctamente.



Figura 115. Pantalla inicial de BASE.

Se deberá ir sobre el enlace "Setup page" que enlazará con el contenido de la figura siguiente. En el nuevo enlace se verá un botón con el texto "Create BASE AG", se seleccionará ahí y se mostrará la figura de la administración para la configuración final. En este último paso se indica que se han creado las tablas adecuadas y sus correspondientes inserciones.

## ANEXO B



No 1

Junio de 2007

### UNIVERSIDAD FRANCISCO GAVIDIA

FACULTAD DE INGENIERIA Y ARQUITECTURA

INGENIERIA EN TELECOMUNICACIONES

### SOLICITUD DE COLABORACIÓN

Somos estudiantes de la facultad de Ingeniería en Telecomunicaciones, y actualmente nos encontramos realizando una investigación de campo sobre el desarrollo de seguridad de los sistemas informáticos en la Universidad Francisco Gavidia.

**NOMBRE DEL PROYECTO:** Diseño y desarrollo de Honeynets Virtuales utilizando VMware, para detección de intrusos informáticos.

**OBJETIVO:** Investigar si existe la factibilidad de realizar el proyecto a través de la encuesta, la cual reflejará la opinión de la Dirección de Tecnología y Comunicaciones de la Universidad Francisco Gavidia.

### INDICACIONES

Marcar con una X en el cuadro correspondiente a su respuesta

1. ¿Conoce usted el riesgo que podrían estar expuestos los sistemas que actualmente poseen a través de las amenazas y/o ataques informáticos?

SI ☐

NO ☐

2. ¿Se ejerce algún tipo de control en contra de estas amenazas?

SI ☐

NO ☐

3. ¿Se ejerce un control de monitoreo periódico y perenne de estas vulnerabilidades?

SI ☐

NO ☐

4. ¿Si su respuesta es afirmativa a la pregunta anterior, favor comente con que periodicidad estas vulnerabilidades son expuestas a sus sistemas?

1 por semana ☐

1 por mes ☐

1 por año ☐

desconoce ☐

5. ¿Tiene usted conocimiento si existe un sistema de seguridad y monitoreo en servidores con servicios públicos en el Internet o la intranet?

SI ☐

NO ☐

6. ¿Le gustaría conocer e implementar un sistema de seguridad con herramientas gratuitas?

SI ☐

NO ☐

7. ¿Le gustaría implementar el control y captura de datos y visualizarlos de forma gráfica como software de monitoreo de ataques al sistema de seguridad?

SI ☐

NO ☐

8. ¿Conoce usted el sistema de seguridad Honeynet con Vmware?

SI ☐

NO ☐

9. ¿Le gustaría conocer una propuesta de diseño de Honeynets Virtuales utilizando VMware, para detección de intrusos y ser implementado en su área?

SI ☐

NO ☐

Si tiene comentarios, favor hacerlos en el siguiente espacio:

---

---

---

DATOS DE PRESENTACIÓN

Fecha: \_\_\_\_\_

Encuestador: \_\_\_\_\_