UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Implementación de un HoneyPot para Análisis Forense

Trabajo de Tesis

para obtener el grado de

Ingeniero en Redes

PRESENTA

Margarita García García

Director de Tesis

Vladimir Veniamin Cabañas Victoria

Asesores

Ing. Rubén Enrique González Elixavide

Dr. Jaime Silverio Ortegón Aguilar

Chetumal, Quintana Roo, México, Marzo de 2012.

UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

Trabajo de Tesis elaborado bajo supervisión del Comité de Asesoría y aprobada como requisito parcial para obtener el grado de:

INGENIERO EN REDES

Comité de Trabajo de Tesis

Director:

M.T.I. Vladimir Veniamin Cabañas Victoria

Asesor:

Ing. Rubén Enrique González Elixavide

Asesor:

Dr. Jaime Silverio Ortegón Aguilar

Chetumal, Quintana Roo, México, Febrero de 2012.

Agradecimientos

Doy gracias…

En primer lugar a mis padres Martin García Razo Y María Sabina García Frayre por el apoyo incondicional.

A mis profesores y en especial al M.T.I. Vladimir Veniamin Cabañas Victoria mi asesor de tesis, quien dedicó tiempo a este trabajo de tesis, con quien pude expresarme claramente y obtener valiosos consejos.

A todos mis compañeros de la carrera que pude conocer a lo largo de 5 años y que al igual que yo pasaron o pasaran tarde o temprano por el mismo proceso.

A esta casa de estudio La Universidad de Quintana Roo de la cual recibí importantes becas y en la que dejo 5 años de la carrera que estoy recorriendo.

Dedicatoria

Dedico este trabajo de tesis enteramente a esas dos personas que Dios me ha dado como ejemplo a seguir, que con paciencia y comprensión, vivieron el proceso del desarrollo de este trabajo, que soportaron mis días de desvelos, que comprendieron las situaciones por las que no los visité y en momentos de angustia me alentaron para al fin poder llegar a este día.

Este logro es por ustedes Martin García Razo y María Sabina García Frayre mis muy queridos y apreciados padres.

Los quiere su *“niña bonita”*.

Resumen

Este trabajo presenta un entorno de red virtual controlado para la instalación y manejo de un servidor Honeypot, así como, se resaltan los beneficios de brindar mayor protección a la información y los métodos que implican su implementación. Se expone el análisis de los datos obtenidos, asi como también se mencionan las herramientas complementarias para cumplir los objetivos planteados.

Se provee un método para identificar las técnicas y estrategias más comunes empleadas en los ataques enfocados en los sistemas informáticos.

Para el desarrollo de este proyecto se aplicó la investigación descriptiva y experimental; cabe mencionar que proyectos de esta índole marcan la pauta para conocer el papel que juega hoy en día la fiabilidad de los sistemas aplicados a la seguridad de la información, tomando en cuenta que este es el cimiento del desarrollo económico, científico y principalmente de la educación.

Es importante hacer mención de los precursores y sus aportes en lo que respecta a los sistemas que abrieron horizontes en la Informática Forense, así como, los medios y técnicas desarrolladas, sin dejar atrás la explicación de la importancia de la información y el gran lazo que la une hoy en día a la tecnología.

Contenido

CAPÍTULO 1
INTRODUCCIÓN

CAPÍTULO 1 INTRODUCCIÓN

El análisis forense es “La técnica de capturar, procesar e investigar información con el fin de que pueda ser utilizada en la justicia”. (McKennish, 1998)

Esta es una de las múltiples definiciones sobre el tema del análisis forense en informática *(Computer forensics*), las cuales abordan aspectos generales y específicos que convergen en todos los casos hacia la identificación, protección, extracción, estudio, interpretación, documentación y exposición de evidencia digital.

La evidencia en la vida real lo es todo, ya que se utiliza para esclarecer hechos y relacionar distintos eventos, la evidencia digital es ademas un elemento en el cual la protección de su legitimidad y veracidad es una tarea que se torna difícil por su frágil naturaleza y vulnerabilidad, esta característica hace a la evidencia digital un constante desafío para aquellos que la analizan en pro del esclarecimiento de cuestiones de vulneración de los sistemas.

Para contar con evidencia digital útil es necesario un dispositivo que haya sido objeto de alguna infracción, esto pone en riesgo la información y a los sistemas que la administran, almacenan y/o procesan; una buena forma de evitar que esto ocurra es la instalación de un servidor *HoneyPot*.

Un *HoneyPot* es herramienta que funciona como una trampa colocada a conciencia, permite simular un estado de vulnerabilidad en un servidor, el cual recolecta todo tipo de muestras con el propósito de realizar un análisis forense de los datos obtenidos, clasificar el tipo de ataque, el origen de éstos, determinar

responsabilidades y en general ayudar en la tarea de prevención de ataques y garantizar la confiabilidad en los servidores auténticos de una organización.

En la ciudad de Chetumal Quintana Roo actualmente no hay registros de la instalación de servidores destinados al análisis y recolección de datos en caso de alguna amenaza; esto se debe a que la infraestructura tecnológica es poca y la ciudad carece de experiencia en el aspecto de la seguridad. Además de los pocos registros de vulneraciones a sistemas de información, no existe un área especializada en análisis forense; sin embargo, la falta de investigaciones en el área de seguridad puede convertir a las instituciones en un punto fácil para ser blanco de ataques.

Es prioritario que las empresas tomen medidas para proteger su información tanto de ataques internos como externos y a todos los niveles, con ayuda de la prevención y el análisis de la evidencia digital.

JUSTIFICACIÓN

Dado el aumento de la importancia de la información en la actualidad, es una tarea fundamental aumentar la confiabilidad en la seguridad y los métodos que implican la implementación de la misma; Honeypot representa un método confiable que se ha desarrollado con grandes expectativas en el camino de la investigación en pro de la seguridad en las redes; la implementación de un servidor Honeypot trae beneficios que pueden marcar la pauta para el fortalecimiento de la seguridad en una red, los cuales permitirán reforzar los conocimientos sobre el comportamiento de los atacantes, así como la prevención de posibles intrusiones a futuro.

La realización de este trabajo tiene la finalidad de aplicar la recolección de datos de un servidor HoneyPot para llevar a cabo un análisis que permita identificar las técnicas y estrategias más comunes empleadas en los ataques en pro de la seguridad en los sistemas de aplicaciones.

HIPÓTESIS

La implementación de un servidor HoneyPot cumpliendo las fases de análisis de comportamiento del servidor, extracción de datos, análisis de resultados, reporte y conclusiones, vinculado al análisis forense permitirá aplicar técnicas de seguridad más confiables.

OBJETIVO GENERAL

Obtener evidencia digital por medio de un servidor Honeypot y comprobar la viabilidad y beneficios que trae consigo la implementación de un servidor de este tipo.

OBJETIVOS PARTICULARES

- Implementación de un servidor HoneyPot.
- Recolección de evidencia digital para análisis forense.
- Definir la rentabilidad del proyecto.

METODOLOGÍA

Se hará un breve análisis de algunas herramientas para implementar HoneyPots, se seleccionará una de acuerdo a criterios que se definan en la presente investigación. Se implementaran herramientas de análisis forense y se realizará un análisis comparativo de los resultados.

Tipo de investigación:

- Descriptiva.
- Experimental

Método utilizado:

- Método Inductivo

Objeto:

- Aplicaciones HoneyPot e investigación de aplicaciones de análisis forense.

Medio:

- Recopilación de información bibliográfica y referencias electrónicas así como también investigación en un entorno controlado.
- Pruebas de ataque simulado al servidor Honeypot y recolección de las evidencias.

En la siguiente tabla se definen las fases del método a seguir en la realización de este proyecto.

Tarea	Descripción
Implementación del servidor HoneyPot	• Instalación del sistema operativo Xubuntu versión 10.04 para la implementación del HoneyPot. • Instalación y configuración de la herramienta Honeyd.
Tiempo de respuesta	Tiempo dedicado para presenciar la llegada de algún intruso.
Análisis del comportamiento del servidor	En caso de actos sospechosos, análisis de la información obtenida.
Extracción de datos	Extracción segura de datos que reflejen el comportamiento del servidor en el período de la infracción.
Reporte	Informe detallado de los acontecimientos y comportamiento del intruso y del servidor.
Conclusiones	Conclusiones del análisis de la evidencia y posibles medidas de seguridad para evitar incidentes a futuro.

Tabla 1 Programa de actividades

CAPÍTULO 2
MARCO TEÓRICO

CAPÍTULO 2 MARCO TEÓRICO

INTRODUCCIÓN

No cabe duda que la tecnología avanza día con día, logrando con esto beneficios sociales evidentes, ejemplo de esto es el rápido desarrollo de las empresas, la educación y la investigación científica y tecnológica; sin embargo este progreso no sólo beneficia a la sociedad, hay que reconocer la existencia de las amenazas y prueba de este hecho son los constantes ataques informáticos y la posibilidad de ocultar las operaciones maliciosas, por mencionar un ejemplo; el acceso a información confidencial es uno de los principales objetivos de los ataques que se presentan en la mayoría de las empresas, compañías y sistemas de educación que han optado por la implementación de tecnología para el manejo de información.

La información en el ámbito social y empresarial es muy importante, es uno de los factores que impulsan el desarrollo de organizaciones e instituciones para la toma de decisiones. Hoy en la era de la información, la tecnología ha permitido adelantos significativos que están introduciéndose en las empresas con cambios imprescindibles, esto con la finalidad de que las organizaciones se adapten a las necesidades de cambio permanente, aprovechando su ventaja competitiva y respondiendo a la necesidad de ser ágil. Al referirse al aspecto de la seguridad existen investigaciones y desarrollos que en la actualidad son de ayuda para la protección de los datos, pero ¿Qué ocurre cuando los métodos de seguridad han sido violados? ¿Cómo detectar las evidencias del ataque?

Actualmente la presencia de expertos en informática que desempeñan tareas como peritos, ha traído un conjunto de teorías, técnicas de análisis y métodos de

prevención para evitar intrusiones, ha sido tanta la demanda de brindar soporte conceptual a la investigación de pruebas generadas y guardadas electrónicamente que estas puedan ser aceptadas en un proceso legal, lo que da como surgimiento a La Informática Forense o *Forensic* como un medio para esclarecer los actos delictivos y fundamentar cada prueba aportada.

LA INFORMÁTICA FORENSE

Según el FBI, la informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. (McKennish, 1998)

La informática forense surge de la necesidad de recrear la secuencia de eventos que han sucedido en un dispositivo digital, la raíz de esta preocupación, fue buscar la prevención, la reacción y corrección a problemas que pudieran afectar los sistemas de información.

Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada. La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales. (Óscar López, 2001)

Se puede decir que evidencia es toda porción de información que permite afirmar o descartar la ocurrencia de un hecho específico y que debe correlacionar todas las posibles variables para no ser circunstancial; al presentar cualquier información que sea considerada evidencia se deben anteponer tres particularidades como son la integridad, autenticidad y confiabilidad, características que se tornan

difíciles de conservar pues tomando en cuenta el Principio de Locard, (principio fundamental en la ciencia forense) que afirma que “cualquiera o cualquier objeto que entra en la escena del crimen deja un rastro en la escena o en la victima”, es decir, cada contacto deja un rastro, este concepto se convierte en el primer enemigo del análisis forense informático pues para obtener la evidencia digital es necesario hacer presencia de herramientas en el escenario que pueden contaminar e invalidar la información.

Los estudios en la informática forense han evolucionado con el avance de la tecnología y existe una gran variedad de herramientas y técnicas que facilitan el estudio y validación de hechos delictivos, una herramienta que se ha desarrollado en pro de la recolección de datos y análisis de agresiones son los “HoneyPot”.

HoneyPot es en sí una trampa colocada a conciencia que permite simular un estado de vulnerabilidad y recolectar todo tipo de muestras (Glasvezel.net, 2011), los HoneyPot son señuelos que permiten la investigación de nuevas técnicas de ataque para comprobar el modus-operandi de los intrusos **fig. 1.**

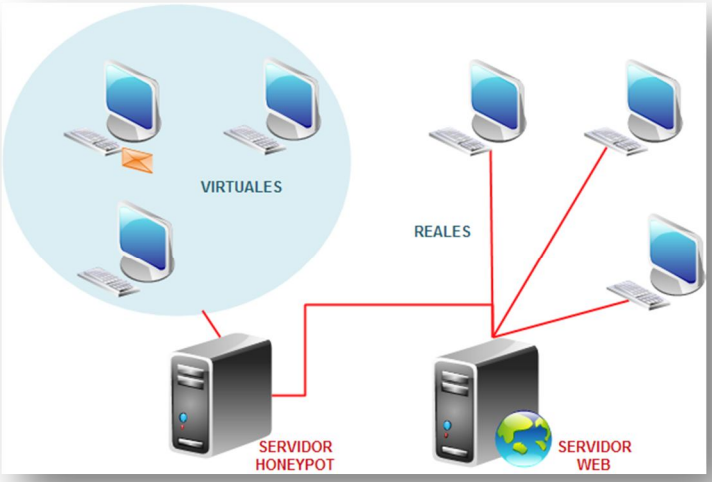

Fig. 1 Ejemplo Honeypot

HoneyPot es un proyecto novedoso, con un potencial enorme para la comunidad informática. Los primeros conceptos fueron introducidos por primera vez por varios

iconos de la seguridad informática, principalmente por Cliff Stoll en el libro "The Cuckoo's Egg" y además de importantes aportaciones de Bill Cheswick en el libro "An Evening with Berferd". Desde entonces, los Honeypots han estado en una continua evolución desarrollándose como una poderosa herramienta de seguridad que ha dado pasos agigantados con ayuda de las contribuciones de los diversos usuarios y ha sido tanto su progreso que han surgido los “Honeynet” herramienta de la comunidad Open Source desarrollada también para ampliar la capacidad de respuesta ante incidentes.

PROYECTOS

En la actualidad existe una larga lista de proyectos muy prometedores relacionados con los Honeypot; por señalar algunos se puede hablar de “Honeyd” de la comunidad Open Source, software de código abierto desarrollado bajo lenguaje C, distribuido bajo la licencia de GNU, publicada por Niels Provos y “Honeynet” organización para la investigación sobre seguridad voluntaria sin fines de lucro que utiliza los Honeypot para recolectar información sobre las amenazas del ciberespacio.

KFSensor es un Honeypot de baja interacción, está basado en una plataforma Windows, cuenta con interfaz gráfica presentando un sistema amigable para el usuario, además de contar con administración remota, tiene una vasta documentación y bajo mantenimiento; identifica patrones de ataque, emula servidores reales como FTP, SMB, POP3, HTTP, Telnet, SMTP y SOCKS, genera informes de la actividad presente pues todo el tráfico TCP, UDP e ICMP es controlado. (KAFSENSOR)

Specter es un Honeypot desarrollado por NetSec, empresa suiza; esta herramienta es de baja interacción, diseñado para un entorno Windows, su objetivo es detectar actividades no autorizadas y obtener información de estas; puede controlar un total de 14 puertos TCP. De estos 14 puertos supervisados, 7

son lo que Specter llama trampas, los otros 7 son lo que llama a los servicios de Specter. (Spitzner, 2003)

Existe una cantidad considerable de personas expertas alrededor del mundo en esta área, sin embargo se reconoce a Dan Farmer y Wietse Venema, los creadores del Forensics Toolkit (kit de herramientas utilizadas en análisis forense) como los pioneros de la informática forense y actualmente, Brian Carrier, autor de varios equipos de herramientas forenses, incluyendo The Sleuth Kit y el navegador de la autopsia forense probablemente como uno de los mayores expertos mundiales en el tema.

CERT

En España existen dos equipos esCERT e IRIS-CERT cuyo director es Manuel Medina, estos organismos fueron creados por el Ministerio de Ciencia y Tecnología a través de la Superintendencia de Servicios de Certificación Electrónica que en conjunto con la Academia tratan de resolver los incidentes informáticos en la Administración Pública, así como difundir información de cómo neutralizar incidentes, tomar precauciones para las amenazas de virus que puedan comprometer la disponibilidad y confiabilidad de las redes.

La Universidad Nacional Autónoma de México (UNAM) cuenta con el Departamento de Seguridad en Cómputo / UNAM-CERT que es el equipo de respuesta a incidentes de seguridad encargado de atender incidentes del dominio.unam.mx y a partir del año 2001 se registró como el único CERT (*Computer Emergency Response Team*) de México reconocido oficialmente ante FIRST (*Forum of Incident Response and Security Teams*) este hecho convirtió a este equipo en el punto clave de contacto para los incidentes en el dominio .mx, además de marcar la pauta para colaborar con entidades del sector gobierno, privado y financiero del país.

Los CERT son organizaciones responsables de recibir, revisar y responder a informes y actividades sobre incidentes de seguridad, cada país suele tener su propio CERT o equipos de respuesta a incidentes, por mencionar algunos, ArCERT de Argentina, US-CERT en Estados Unidos, UNAM CERT en México, CERT Chile, Open Source CERT, CERT India y CERT Australia.

DIFUSIÓN

Andrés Velázquez, consultor en México de seguridad informática y cómputo forense, es uno de los tres expertos en cómputo forense de América Latina, quien asegura que cada vez más organizaciones se interesan por las acciones y resultados de esta disciplina en la que ha trabajado desde hace años.

Ha sido tanta la demanda del desarrollo de herramientas y proyectos que fortalezcan esta área de la informática que el avance es notorio y ha sido posible gracias a la ayuda y apoyo de la industria del sector privado y público. El progreso se ve reflejado en los libros publicados, los informes y artículos sobre este tema mencionando también a los proyectos y herramientas desarrolladas.

Documentación de los Procedimientos de Análisis Forense de Computadores es el título del artículo publicado en la revista On-Line de Criminalística Ciencia Forense.cl y escrito por Jhon J. Bárbara, Supervisor del laboratorio de análisis de delitos en el Departamento de Aplicación de la Ley (FDLE) en Tampa Florida, en el cual aborda un tema de suma importancia para el análisis forense digital, que es la documentación de la técnica de Procedimientos Operativos Estándar (SOP) para el análisis de los medios digitales.

El 21 de noviembre del año 2005 tuvo lugar el 3er congreso iberoamericano de seguridad informática en la Universidad Técnica Federico Santa María de Chile, en el cual se presentó una ponencia denominada *"Implementación y Definición del Modo de Empleo de la Informática Forense"* impartida por Héctor Gómez Arraigada de la armada de Chile, quien explicó temas como la toma de conciencia, los problemas en investigaciones y la implementación de esta disciplina.

La Segunda edición del Libro en línea titulado *Análisis Forense Digital* publicado en junio del 2007 y cuyo autor es Miguel López Delgado, explica como la aplicación de técnicas forenses al análisis de sistemas proporciona una metodología adecuada en el proceso de respuesta ante incidentes, además de hacer incursión en el apasionante y novedoso mundo del Análisis Forense Digital.

La revista internacional *Journal of Digital Evidence* es una de las cuales se dedica a publicar artículos relacionados con la evidencia digital, por mencionar uno, el artículo *"Computer Forensic Analysis in a Virtual Environment"* publicado en el año 2007 donde analizan el comportamiento de la fase del análisis para investigaciones en computación forense en un ambiente virtual utilizando la herramienta VMWare.

El artículo titulado *El Análisis Forense En Dispositivos Móviles y Sus Futuros Riesgo* publicado el 10 de abril 2008 en la Revista Digital Universitaria de la UNAM y escrito por Israel Becerril Sierra, Especialista de seguridad informática en sistemas Unix UNAM-CERT, aborda temas relacionados con el análisis forense aplicado a dispositivos móviles, además de predecir las estrategias que los intrusos estarán usando para vulnerar un dispositivo móvil y afectar a sus usuarios, entre otros puntos hace énfasis en la evolución que tendrán los virus y gusanos para infectar dispositivos móviles que puedan ser usados con fines maliciosos.

Uno de los artículos que aporta una interesante reflexión sobre el nivel de calidad y confiabilidad de las herramientas de la primera generación, ofreciendo al lector una serie de criterios para que la segunda generación de herramientas forenses pueda cumplir sus nuevos objetivos, es sin duda el artículo titulado *A Second Generation Computer Forensic Analysis System* publicado en la edición 2009 del *Digital Forensic Research Workshop*.

Una revista más que ha dado importancia a esta rama de la informática por medio del enfoque al análisis forense de imágenes digitales es Signal Processing

Magazine de la IEEE, la cual en la edición de Marzo 2009 se describió la Detección de falsificaciones en imágenes, métodos basados en pixeles, en formato, en cámara, en la geometría, en la física y ambiente en el artículo titulado *Image Forgery Detection.*

Helena Fuentes, directora del Departamento Legal del Grupo Winterman, publicó un artículo el 24 de Noviembre del año 2009, titulado *Introducción a la Prueba Digital y al Análisis Forense Informático*, en el cual hace una pequeña introducción a los aspectos generales que intervienen en una disciplina tan interesante como lo es el análisis forense.

La revista PCWORLD PROFESIONAL ha dado un enfoque importante al análisis forense digital, prueba de esto es una de los artículos que presentó el 01 de Marzo del año 2009, titulado *"Análisis forense. Cómo investigar un incidente de seguridad"* escrito por Óscar Delgado Mohatar y Gonzalo Álvarez Marañón, colaboradores del Grupo de Investigación en Criptología y Seguridad de la Información del CSIC, en el cual se aborda el tema como una de las fases más importantes de la respuesta a incidentes que consiste en la investigación del incidente para saber por qué se produjo la intrusión, quién la perpetró y sobre qué sistemas, en este artículo se presentan las características más destacadas del análisis forense.

Un trabajo más que aporta a esta área es el libro *"Análisis Forense Digital en sistemas Microsoft Windows"* de Juan Garrido Caballero mejor conocido como "Silverhack" y publicado en Julio de 2009 en el cual se puede encontrar una gran cantidad de información de las revisiones que se hacen de decenas de aplicaciones, desde su uso más sencillo hasta su funcionamiento a bajo nivel, aportando un inventario completo de tareas a llevar a cabo en Windows.

El libro *Hacking: The Next Generation* de Nitesh Dhanjani, Billy Ríos y Brett Hardin publicado en el año 2009 introduce al lector en el mundo de los phishers, para ayudar a conocer mejor sus motivaciones y su comportamiento, esta obra es una

gran contribución, pues se convierte en un apoyo en la realización del análisis forense digital.

ESTÁNDARES EN LA INFORMÁTICA FORENSE

La Informática forense es una ciencia relativamente nueva y no existen estándares aceptados. Existen proyectos que están en desarrollo como el C4PDF de Roger Carhuatocto Código de Prácticas para Forencia Digital que no es más que un manual basado en criterios siguiendo el asesoramiento de la comunidad y expertos, el Open Source Computer Forensics Manual, de Matías Bevilacqua Trabado y las Training Standards and Knowledge Skills and Abilities de la IOCE (International Organization on Computer Evidence) (Rivera), organismo internacional fundado en el año de 1995, compuesto por agencias gubernamentales y cuyo propósito es realizar un foro internacional sobre investigaciones de evidencia digital y temas de computación forense; sin embargo, todavía hay un largo camino que recorrer en esta área de la informática que no ha sido cubierta del todo y es un arduo trabajo el cual debe ser realizado pues la creación y aceptación de un estándar es difícil y aún más si se trata de un tema de naturaleza tan delicada, flexible y frágil.

Para que todo lo realizado en la informática forense sea exitoso, es necesario que se tengan regulaciones jurídicas que penalicen a los atacantes y que sea posible asignar una sentencia por los crímenes cometidos. Cada país necesita reconocer el valor de la información de sus habitantes y poder protegerlos mediante leyes.

SISTEMA OPERATIVO

El sistema operativo a instalar es XUBUNTU 10.04 distribución de software libre en su versión 10.04 con mayor soporte, más reciente, procedida de Ubuntu y más ligero.

Xubuntu fue desarrollado en el año 2006 con el objetivo de producir una distribución amigable para el usuario aunando la usabilidad y rendimiento además de hacer hincapié en el uso mínimo de memoria; logrando esto con la integración del entorno de escritorio Xfce que se caracteriza por ser un entorno ligero, diseñado para la productividad; Xfce carga y ejecuta aplicaciones rápidamente conservando recursos del sistema. (Xubuntu, 2011)

Xubuntu está diseñado pensando en la seguridad ya que recibe actualizaciones de seguridad gratuitas por lo menos durante 18 meses y con Long Term Support (LTS) se recibe apoyo de tres años.

Dadas las características del sistema, el gran soporte y los requerimientos mínimos es ideal para alcanzar uno de los objetivos del proyecto que consiste en implementar un sistema de alarma y distracción de bajo costo.

XUBUNTU 10.04 REQUISITOS MÍNIMOS	
RAM	256 MB
DISCO DURO	2 GB

Tabla 2 Requisitos para instalar Xubuntu

HONEYPOT

En el siguiente apartado se explican los por menores de las aplicaciones que se complementan con la instalación del Honeypot.

HONEYD

Del autor Niels Provos, publicado en el año 2002, bajo la licencia de GNU y desarrollado bajo el lenguaje C; esta herramienta tiene la capacidad de crear hosts virtuales con distintos sistemas operativos que pueden ser configurados para ejecutar servicios arbitrarios, permite a un único host reclamar varias direcciones IP, además de fortalecer la seguridad disuadiendo a los atacantes al ocultar los sistemas reales por medio de sistemas virtuales. (Provos, 2008)

Soporta servicios mediante la aplicación de subsistemas como UNIX, esto en el espacio de direccionamiento IP, permitiendo que cualquier aplicación de red se enlace dinámicamente para crear conexiones TCP y UDP y así poder crear un ambiente lo más real posible; esto con la finalidad de engañar al intruso.

Toda configuración de los sistemas a simular se encuentran en un archivo con distintos bloques de código que especifican las características del sistema, es decir el sistema operativo o personalidad que tendrá, los servicios habilitados y los puertos que serán cerrados o en determinada situación abiertos; las diferentes personalidades TCP se aprenden de la lectura de un archivo de huellas dactilares nmap, archivo ubicado en la ruta **/etc/honeypot/nmap.assoc.**

Honeyd permite rutas asimétricas y la integración de los equipos físicos en la topología de la red virtual. Como resultado, es posible utilizar Honeyd para las simulaciones de red; un beneficio adicional de este enfoque es la capacidad de los Honeypot para crear el tráfico de fondo eventual como las páginas web y correo electrónico solicitando la lectura.

Honeyd se puede utilizar para crear una red virtual de “miel” o de supervisión general de la red. Apoya la creación de una topología de red virtual dedicada incluidas las rutas y los routers. Las rutas se pueden atribuir a la pérdida de paquetes y latencia para que la topología se torne más real.

FARPD

Herramienta que permite escuchar las peticiones ARP y dar respuesta a las direcciones IP que no han sido asignadas; esta herramienta es utilizada a la par con Honeyd que si bien este crea host virtuales, ARPD rellenará el espacio de direcciones IP que no han sido asignadas en la red, dando al intruso información falsa respecto a las direcciones asignadas realmente (Comunidad Ubuntu, 2011).

CAPÍTULO 3
DESARROLLO

CAPÍTULO 3 DESARROLLO

IMPLEMENTACIÓN DE HONEYD

La implementación de la herramienta Honeyd se lleva a cabo como se indica en los siguientes pasos:

Instalación de la herramienta Honeyd

Dada la distribución seleccionada para el desarrollo del proyecto, la implementación de la herramienta **Honeyd** se torna sencilla, ya que esta herramienta es considerada como un paquete **Synaptic** que puede ser añadido al sistema en 3 pasos:

1. Ubicarse en el panel y desplegar el menú de **Aplicaciones>> Sistema>>Gestor de Paquetes Synaptic, fig. 2.**

Fig. 2 Menú aplicaciones

a. Tras realizar las instrucciones anteriores, el sistema pide introducir la contraseña, esto por medida de seguridad ya que instalar un paquete de Synaptic es considerado por el sistema como una tarea administrativa en la cual es posible modificar partes esenciales del sistema **fig. 3.**

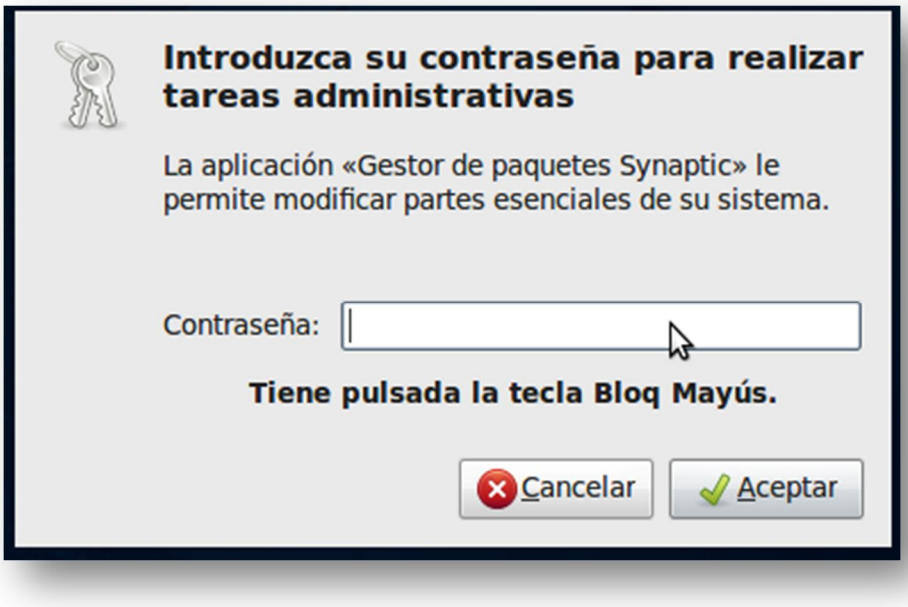

Fig. 3 Comprobación para tareas administrativas

b. Una vez ubicado el **Gestor de Paquetes Synaptic** el último procedimiento es buscar los paquetes **Honeyd** y **Honeyd-common fig.4**, seleccionar los antes mencionados e instalarlos dando clic derecho, cabe mencionar que este proceso tarda algunos minutos.

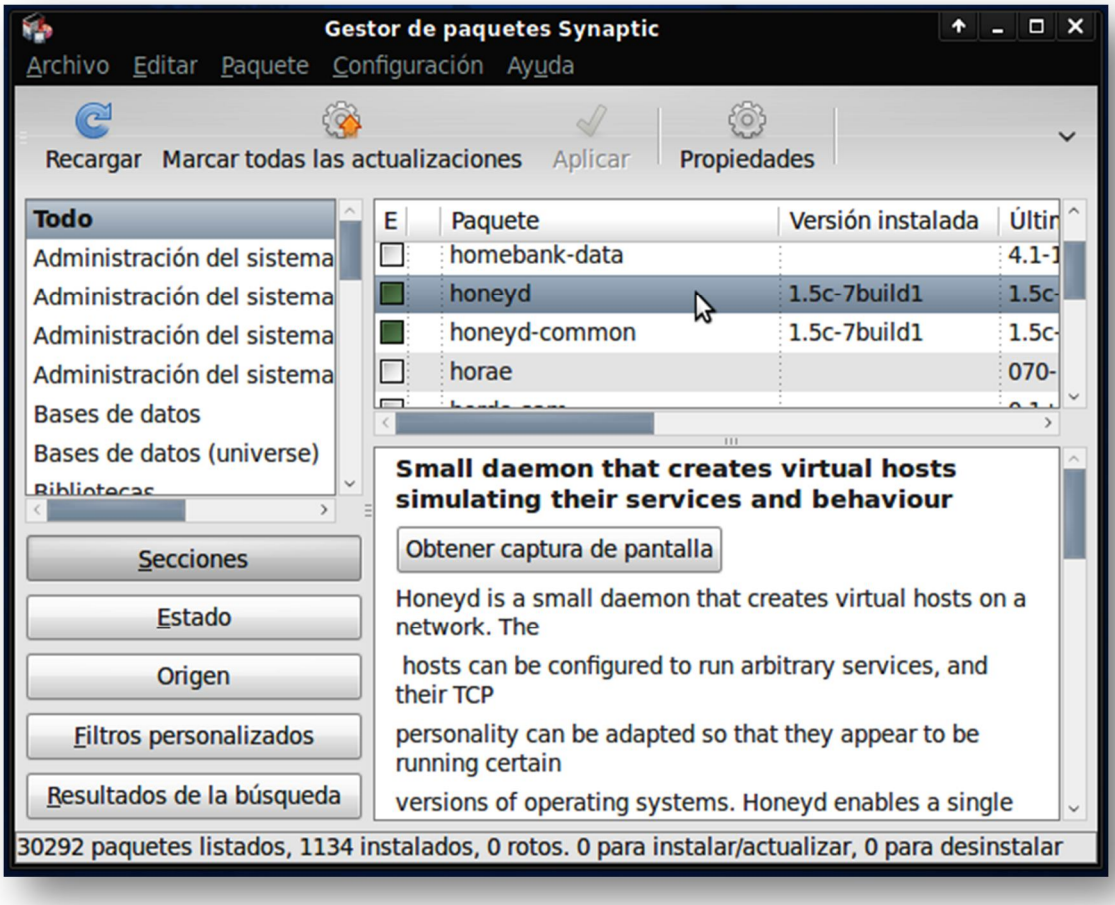

Fig. 4 Gestor de Paquetes Synaptic

CONFIGURACIÓN DE DIRECCIÓN IP

Para configurar la dirección de red es necesario ubicar el icono de red **fig**. **5**, desplegar el menú con un clic secundario y seleccionar la opción configurar conexiones de red, automáticamente se abre la ventana de conexiones de red, la cual cuenta con varias pestañas de entre las cuales se encuentra la denominada Cableada (fig.5), en esta pestaña se encuentra por default creada la conexión Auto eth0, esta conexión es la que se configurará, en este caso, para asignar una dirección IP al servidor.

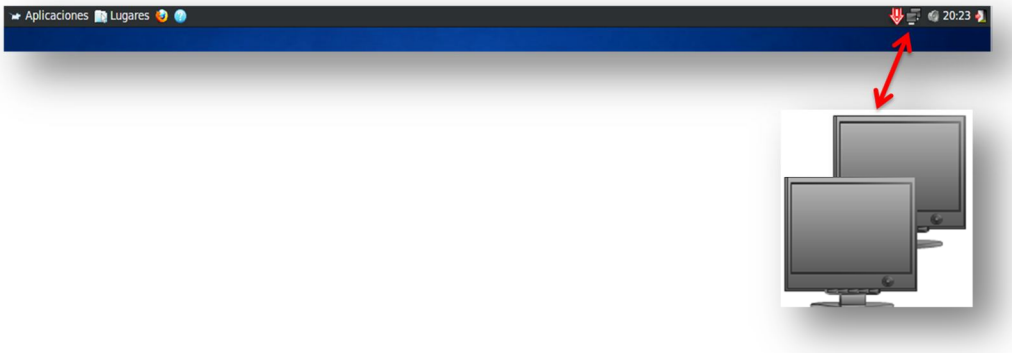

Fig. 5 Configurar dirección de red

Una vez seleccionada la conexión Auto eth0 hay que configurar la dirección IP, para esto es necesario dar doble clic, acto seguido se abre la ventana para editar la conexión, el primer parámetro es el método por el cual se asigna la dirección IP, se despliega la lista y se selecciona el método manual, dado que la tarea del sistema es fungir como un servidor es necesario asignar una dirección estática; en el penúltimo paso se definieron los siguientes parámetros Tabla 3:

Dirección	Máscara de red	Puerta de enlace
	Clase C	
182.168.17.xxx	255.255.255.0	182.168.17.254

Tabla 3 Parámetros para dirección IP

El último paso es Aplicar los cambios realizados en la configuración de la conexión de red y reiniciar el servicio con el siguiente comando:

```
sudo /etc/init.d/networking restart
```

CONFIGURACIÓN DE HONEYD

Para configurar Honeyd existe un archivo de vital importancia en el cual residen los datos y parámetros que definen el comportamiento del Honeypot, es el archivo **honeyd.conf** en el que se delimitan las características que tienen los equipos y servidores simulados para fungir como distractores para los posibles intrusos.

Al instalar Honeyd en el sistema se crea automáticamente un archivo honeyd.conf que contiene configuración predeterminada, este archivo se modifica de acuerdo a las características de los equipos que se desean simular, a continuación se presenta como ejemplo una posible configuración de un host:

```
create default
set default personality "FreeBSD 2.2.1-STABLE"
set default default tcp action reset
add default tcp port 80 open
add default tcp port 22 "sh scripts/web.sh"
add default tcp port 113 reset
add default tcp port 1 reset
```

Create.- Parámetro que se utiliza para definir el nombre que tendrá el host a simular, en este caso la personalidad definida es *default*.

Set.- Parámetro que se utiliza para asignar el sistema operativo que simula el host creado, en este caso el sistema asignado es “FreeBSD 2.2.1-STABLE”, los sistemas operativos y las versiones disponibles que son posibles de asignar se encuentran en el archivo ubicado en la ruta /etc/honeypot/nmap.assoc.

Default.- Parámetro que indica el protocolo a utilizar, en este caso es TCP (**Transport Control Protocol),** sin embargo también es posible asignar los protocolos **UDP** e **ICMP.**

Action.- Parámetro que determina el comportamiento del puerto, el parámetro *reset* significa que este puerto responde con un RST, que de acuerdo con la especificación TCP RFC793 se devuelve un paquete RST cuando se intenta

conectar a un puerto sin servicio; en la siguiente tabla se especifican los posibles comportamientos de los puertos Tabla4.

PROTOCOLO	COMPORTAMIENTO	ESPECIFICACIÓN
TCP (Por default está abierto)	**OPEN**	**Responde con SYN/ACK para establecer conexión.** • El indicador SYN de TCP representa un pedido para establecer una conexión. • El indicador ACK indica que el paquete es un acuse de recibo.
TCP (Por default está abierto)	**BLOCK**	**El paquete se pierde y no hay respuesta.**
TCP (Por default está abierto)	**RESET**	**Significa que este puerto responde con un RST, que de acuerdo con la especificación TCP RFC793 se devuelve un paquete RST cuando se intenta conectar a un puerto sin servicio.**
UDP (Cerrado por default)	**OPEN**	**No hay respuesta.**
UDP	**BLOCK**	**El paquete se pierde y no hay**

(Cerrado por default)		**respuesta.**
UDP (Cerrado por default)	**RESET**	**Responde con un mensaje ICMP de error de puerto.**
ICMP (Abierto por default)	**OPEN**	**Responde con paquetes ICMP.**
ICMP	**BLOCK**	**El paquete se pierde y no hay respuesta.**

Tabla 4 Protocolos, comportamiento y especificación

add default tcp port 80 open. - Esta línea indica el número de puerto y el estado en el que se encuentra dicho puerto.

"sh scripts/web.sh".- Esta línea indica que se utiliza un script para simular determinada acción, en este caso el script web.sh simulará servicios web; los scrips disponibles se encuentran ubicados en la ruta /usr/share/honeyd/script; cabe mencionar que para poder utilizar los scripts es necesario asignar privilegios al directorio en el cual se encuentran, esto se logra con la siguiente línea de comandos:

chmod 777 cd /usr/share/honeyd/scripts/

Una vez puntualizados los parámetros del archivo de configuración de honeyd, se presenta el archivo de configuración del servidor real:

```
create windows

set windows personality "Microsoft Windows XP Professional SP2"
```

```
set windows default tcp action reset
set windows default udp action reset
set windows default icmp action open
add windows tcp port 23 “perl /usr/share/honeyd/scripts/faketelnet.pl”
add windows tcp port 80 “sh /usr/share/honeyd/scripts/web.sh”
add windows tcp port 139 open
add windows udp port 137 open
add windows tcp port 137 open

bind 192.168.17.140 windows

create windows2

set windows2 personality "Microsoft Windows XP Professional SP2"
set windows2 default tcp action reset
set windows2 default udp action reset
set windows2 default icmp action open
add windows2 tcp port 139 open
add windows2 udp port 137 open
add windows2 tcp port 137 open
bind 192.168.17.150 windows2


create sticky
set sticky personality “Apple Mac OS 8.6”
set sticky default tcp action tarpit open
set sticky default udp action block
bind 192.168.17.110 sticky
```

Se simulan 3 computadoras con las siguientes características:

```
set windows personality "Microsoft Windows XP Professional SP2"
```

Como se puede observar en la línea anterior la computadora simulará un sistema operativo Microsoft Windows XP Professional y service pack 2.

```
set windows default tcp action reset
```

Esta línea indica que el protocolo TCP responderá con el bit RST lo que significa el rechazo del intento de conexión.

```
set windows default udp action reset
```

En el caso de la línea anterior el protocolo UDP responde con un mensaje ICMP de error de puerto.

```
set windows default icmp action open
```

En el caso de ICMP en acción OPEN responderá con paquetes ICMP.

```
add windows tcp port 23 “perl /usr/share/honeyd/scripts/faketelnet.pl”
```

Esta línea indica el protocolo tcp y puerto 23 por el cual se simulará las respuestas a peticiones de conexión telnet, el script aplicado es faketelnet es utilizado para simular respuestas a conexiones telnet en sistemas Windows, Linux y Solaris.

```
add windows tcp port 80 “sh /usr/share/honeyd/scripts/web.sh”
```

La línea anterior indica que por el puerto 80 se realizará la simulación de un servidor web, utilizando en este caso el script web.sh.

```
add windows tcp port 139 open
add windows udp port 137 open
add windows tcp port 137 open
```

Las líneas anteriores indican los puertos adicionales que se mantendrán abiertos en esta máquina.

Tras haber configurado el archivo *honeyd.conf* se instalarán dos de las herramientas que complementan el trabajo de la aplicación *honeyd*, las aplicaciones son:

1. *FARPD*.- FARPD rellenará el espacio de direcciones IP que no han sido asignadas en la red, dando al intruso información falsa respecto a las direcciones asignadas.
   Para instalarlo se agrega la siguiente línea de comandos en una terminal.

   ```
   sudo apt-get install farpd
   ```

2. *NMAP.-* Hay otro archivo importante en el honeyd que es el nmap.prints, este archivo guarda las huellas de nmap. Nmap usa este archivo para validar el sistema operativo de un equipo remoto y honeyd lo usa para emular la pila de protocolos IP para ese sistema operativo, de esta manera es posible ir actualizando la lista con nuevos sistemas operativos.

   Para instalarlo se agrega la siguiente línea de comandos en una terminal.

```
sudo apt-get install nmap
```

Una vez instaladas las aplicaciones necesarias se procede a su aplicación y finalmente el inicio de *honeyd* en el sistema.

Se aplica FARPD a todo el segmento de red en el que actúa *honeyd*.

```
farpd 192.168.17.0/24
```

Para poder registrar todas las alarmas que se presentan es necesario tener un archivo de bitácora -log el cual es de suma importancia, dado que de este archivo se obtendrá la información que se analizará y permitirá llegar a conclusiones importantes en este proyecto, dicho archivo se crea en la ruta /var/log/honeypot/ con el siguiente comando:

```
nano /var/log/honeypot/honeyd.log
```

Como último paso queda iniciar el servicio de *honeyd*, añadiendo la siguiente línea de comandos en una terminal:

```
honeyd -i eth0 -d -p nmap.prints -l /var/log/honeypot/honeyd.log -f honeyd.conf
192.168.17.140 192.168.17.150 192.168.17.11
```

Parámetros:

-i.- Este parámetro indica la interfaz por la cual se iniciará el servicio en este caso es la **eth0**

-d.- Este parámetro habilita el envío de mensajes en modo verboso.

-p (fingerprints).- Este parámetro lee las huellas dactilares estilo nmap.

−l (logfile).- Registrar los paquetes y las conexiones con el archivo log del sistema.

−f (file).- Este parámetro permite tener acceso al archivo de configuración para la simulación de distintos sistemas operativos.

Una vez instalado el servidor *Honeypot* se procede a levantar los servidores reales en este caso un servidor web y un servidor de correo, la configuración y el ambiente creado se puede apreciar en la **fig. 6** es posible visualizar la configuración de estos servidores en el **anexo número 1.**

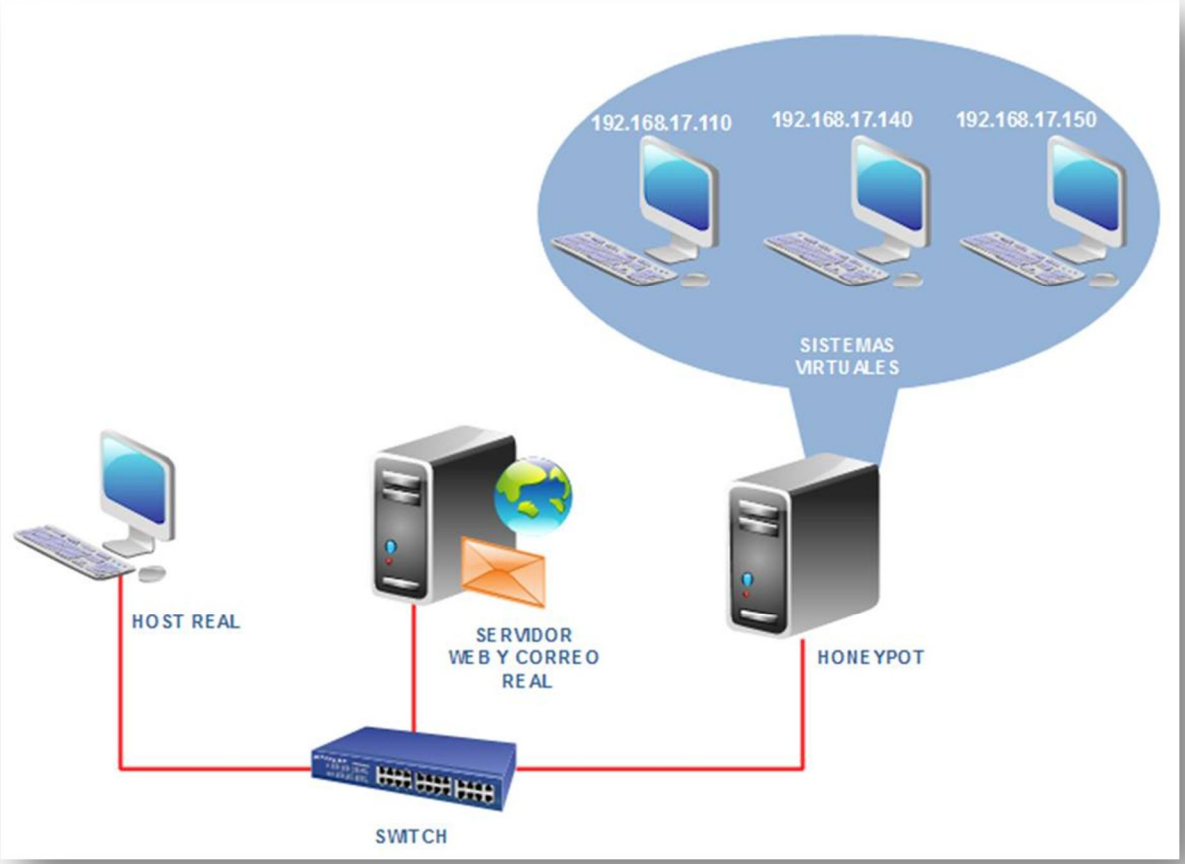

Fig. 6 Ambiente diseñado para el proyecto

CAPÍTULO 4
PRUEBAS Y CONCLUSIONES

CAPÍTULO 4 PRUEBAS

La fase de pruebas consistio en mantener al servidor con todos lo servicios levantados para realizar pequeñas pruebas y asegurar la disponibilidad de los servicios.

Para el cuarto día y utilizando el resultado de la investigación de **Nely Cristina Martínez Aguilar**, quien sometió al *Honeypot* instalado a una serie de pruebas y ataques de intrusión; para lo cual ahora hay que realizar el análisis de la actividad presentada en el sistema y descubrir qué tipo de ataque se perpetro, o cuales puertos fueron dirigidos y la posible herramienta o herramientas utilizadas.

Para el análisis de las pruebas obtenidas a través de los archivos de registro log fue necesario la instalación de ***Honeydsum*** (analizador de registros), esta herramienta fue desarrollada por el equipo brasileño Honeynet, escrita en Perl; esta herramienta estuvo sujeta a prueba bajo un sistema OpenBSD 3.4 y Linux Slackware versión 9.1, con Perl 5.8.0 y con registros de *honeyd* de las versiones 0.7 y 0.8, estos resúmenes pueden ser generados aplicando distintos parámetros, filtrando por puertos, protocolos, direcciones IP o redes; es capaz de identificar la dirección principal, el puerto al que se realizó la conexión y el número de conexiones realizadas por hora, además de generar gráficos de los resultados arrojados. (Honeynet.BR Project, 2008)

Para la instalación de *honeydsum* fue necesario cubrir los siguientes requisitos:

REQUISITOS PARA INSTALAR HONEYDSUM
Perl
Módulo Net::Mask para Perl
Módulo GD para Perl
Módulo GD::Graph::pie para Perl
Módulo GD::Graph::bars para Perl
Módulo GD::Graph::bars3d para Perl

Tabla 5 Requisitos para instalar Honeydsum

Una vez instalados los modulos descritos se procede a realizar en análisis del archivo log generado durante el tiempo que se presentó actividad maliciosa en el *honeypot*, para iniciar el analizador *Honeydsum* sólo hay que introducir la siguiente línea de comandos en una terminal:

```
./honeydsum.pl -c honeydsum.conf [-hV] log-archivo1 log-archivo2... log-archivox
```

Donde el significado de los parámetros utilizados es el siguiente:

PARÁMETROS	
-c	Indica el nombre del archivo bajo el cual se analizarán los registros.
-h	Muestra la opción de ayuda.
-V	Permite visualizar el número de versión.
-w	Muestra los resultados en pantalla como una página web.

Tabla 6 Parámetros

Los primeros datos arrojados son la cantidad total de conexiones intentadas; en la primera ocasión se detectaron 97 conexiones, en la segunda incidencia fueron detectadas **172** y en la última en la que se detectó la mayor cantidad de conexiones en un lapso de tiempo sumamente corto el número de conexiones detectadas fue **137328.**

CONTADOR DE CONEXIONES 1a INCEDENCIA	
Total	97
TCP	3
UDP	7
ICMP	87

Tabla 7 Contador de conexiones 1a incidencia

CONTADOR DE CONEXIONES 2da INCEDENCIA	
Total	172
TCP	3
UDP	50
ICMP	119

Tabla 8 Contador de conexiones 2a incidencia

En el ataque número 3 no fue posible identificar cuantas conexiones fueron realizadas de acuerdo al protocolo ya que al tomar en cuenta que la instalación se realizó en un equipo de baja capacidad de almacenamiento y procesamiento, en la última incidencia la gran cantidad de conexiones realizadas provocó la inhabilitación del sistema y con esto la desconexión del Honeypot por un lapso no mayor de 10 minutos.

La información del tercer ataque presentado es sumamente extensa el cual se presenta en el anexo A.

En la siguiente tabla se muestran las 10 conexiones con mayor ocurrencia en la incidencia número 3, así como también el puerto y la cantidad de conexiones realizadas.

NÚMERO	DESTINO	NÚM. DE CONEXIONES
1	137/TCP	25
2	80/TCP	16
3	139/TCP	15
4	445/TCP	9
5	8/ICMP	9
6	161/UDP	8
7	23/TCP	8
8	135/TCP	7
9	33381/UDP	7
10	81/TCP	7

Tabla 9 Las 10 conexiones con mayor ocurrencia en la incidencia número 3

A continuación se muestran los resultados obtenidos en las 2 primeras incidencias especificado por cada sistema simulado, incluyendo cantidad de conexiones intentadas, puerto al que fueron dirigidas y las direcciones que fueron autoras de dicha actividad.

Actividad identificada en el sistema simulado con la dirección 192.168.17.110.

INCIDENCIA NÚM. 1 **Honeypot: 192.168.17.110**		
Dirección fuente IP	Destino	Núm. De conexiones
31.86.191.30	8/icmp	1
73.122.183.94	8/icmp	1
192.168.17.21	33381/udp	3
	80/tcp	3
249.185.62.5	8/icmp	1
IPs	**Resources**	**Connections**
4	3	9

Tabla 10 Resumen 1 de actividad identificada

INCIDENCIA NÚM. 2 Honeypot: 192.168.17.110		
Dirección fuente IP	Destino	Núm. De conexiones
169.254.90.77	137/udp	15
	3/icmp	5
	8/icmp	25
192.168.17.21	33381/udp	9
	80/tcp	3
	8/icmp	19
192.168.17.68	8/icmp	15
IPs	**Resources**	**Connections**
3	5	91

Tabla 11 Resumen 2 de actividad identificada

Analizando la información presentada en las tablas **10** y **11** se encontraron varias coincidencias; la dirección 192.168.17.21 realizó intentos de conexión en ambas ocasiones, en la primera incidencia realizó 2 conexiones y en la segunda 3 y ambas conexiones fueron dirigidas a los destinos 33381/udp y 80/tcp; además de que en la cantidad de conexiones realizadas al puerto 80/tcp es el mismo en las dos incidencias.

En lo que respecta a las demás conexiones realizadas las direcciones autoras no se encuentran en nuestro segmento excepto 192.168.17.68 la cual realizó 15 conexiones dirigidas al puerto 8/icmp destino con mayor ocurrencia de conexiones presentadas en el sistema con dirección 192.169.1.110.

Actividad identificada en el sistema simulado con la dirección 192.168.17.140

INCIDENCIA NÚM. 1 Honeypot: 192.168.17.140		
IP fuente	Destino	Conexiones
103.250.237.87	8/icmp	1
107.89.153.93	8/icmp	1
115.139.102.107	8/icmp	1
116.207.59.50	8/icmp	1
117.53.118.104	8/icmp	1
126.60.197.43	8/icmp	1

134.68.89.86	8/icmp	1
137.230.173.123	8/icmp	1
138.75.152.119	8/icmp	1
140.29.96.120	8/icmp	1
145.84.112.127	8/icmp	1
146.157.137.30	8/icmp	1
149.126.27.6	8/icmp	1
149.242.30.102	8/icmp	1
155.203.85.116	8/icmp	1
157.227.117.96	8/icmp	1
160.214.185.42	8/icmp	1
163.200.134.3	8/icmp	1
170.26.224.55	8/icmp	1
18.176.174.23	8/icmp	1
182.162.194.121	8/icmp	1
182.163.187.40	8/icmp	1
192.168.17.21	33381/udp	2
204.35.198.77	8/icmp	1
206.34.40.32	8/icmp	1
222.240.197.9	8/icmp	1
226.3.155.52	8/icmp	1
230.152.80.59	8/icmp	1
230.252.218.18	8/icmp	1
233.136.186.122	8/icmp	1
236.249.66.33	8/icmp	1
238.208.84.78	8/icmp	1
239.184.97.98	8/icmp	1
240.205.70.11	8/icmp	1
243.184.126.127	8/icmp	1
248.41.154.51	8/icmp	1
25.228.17.66	8/icmp	1
254.216.99.112	8/icmp	1
255.144.70.25	8/icmp	1
27.88.47.121	8/icmp	1
29.10.114.25	8/icmp	1
30.20.6.27	8/icmp	1
37.54.134.7	8/icmp	1
41.152.214.101	8/icmp	1
43.147.196.33	8/icmp	1
49.250.91.40	8/icmp	1
5.149.177.94	8/icmp	1
67.87.0.94	8/icmp	1

70.3.22.44	8/icmp	1
75.32.98.109	8/icmp	1
77.121.78.102	8/icmp	1
79.34.244.104	8/icmp	1
81.202.85.45	8/icmp	1
81.216.106.119	8/icmp	1
83.127.60.54	8/icmp	1
86.156.6.77	8/icmp	1
86.164.181.85	8/icmp	1
86.217.109.23	8/icmp	1
9.203.158.19	8/icmp	1
95.61.169.74	8/icmp	1
96.248.148.84	8/icmp	1
IPs	**Resources**	**Connections**
61	2	62

Tabla 12 Resumen 3 de actividad identificada

INCIDENCIA NÚM. 2 **Honeypot: 192.168.17.140**		
IP fuente	Resource	Conexiones
169.254.90.77	137/udp	5
	3/icmp	2
	8/icmp	15
192.168.17.21	33381/udp	9
	8/icmp	6
192.168.17.68	8/icmp	5

IPs	**Resources**	**Connections**
3	4	42

Tabla 13 Resumen 4 de actividad identificada

Al seguir la misma línea de análisis se busca la presencia de la dirección 192.168.17.21 que en la información obtenida respecto a las conexiones presentadas en el sistema con la dirección 192.168.17.140 también presentó actividad en las dos incidencias, en la primera sólo realizó dos conexiones al destino 33381/udp, destino que coincide en la segunda incidencia sólo que a diferencia de la primera en la segunda fase esta dirección realizó 15 conexiones, 9 de ellas dirigidas al destino 33381/udp y las 6 restantes dirigidas al destino 8/icmp;

cabe mencionar que al igual que en el sistema con la dirección 192.168.17.110 el destino 8/icmp fue el que presentó mayor ocurrencia.

Respecto a las demás direcciones sólo la 192.168.17.68 se encuentra en el segmento en el que se está trabajando es por eso que es posible iniciar un bosquejo de los que se intentaba realizar en los ataques, además de mencionar que la conexiones tal vez fueron realizadas con algún programa con el cual es posible ocultar la dirección real, uno de ellos pueden ser:

1. ***Nmap*-** Herramienta de exploración de redes y de sondeo de seguridad / puertos; es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos. (Lyon, 1997)

2. ***Smurf*-** Este ataque envía paquetes ICMP (ping) *spoofeados* con direcciones de una máquina de la misma red o con la dirección fuente de la misma víctima, por lo tanto, se contesta el ping hacia sí misma y comienza una inundación de paquetes y la máquina termina saturándose al consumirse el ancho de banda. (Borghello, 2009)

3. ***ICMP echo reply attack*-** Similar al *smurf*, pero sin enviar datos *spoofeados* y por lo tanto, sería necesario tener una conexión mayor o igual para lograr hacer algo contra un sitio con un gran ancho de banda.

4. **MIX-** Es un ataque combinado, envía paquetes UDP, SYN e ICMP.

5. **TFN2K-** Es una herramienta que permite explorar recursos en blancos señalados por ejemplo: Plataformas de UNIX, Solaris, de Windows NT y las que estén conectadas a Internet. Los ataques pueden ser directa e indirectamente a la víctima, los paquetes

pueden ser enviados de una forma aleatoria utilizando TCP, UDP e ICMP. (McAfee, 2003-2011)

Actividad presentada en el sistema simulado con la dirección 192.168.17.150

INCIDENCIA NUM. 1 Honeypot: 192.168.17.150		
IP fuente	Resource	Conexiones
0.147.73.76	8/icmp	1
4.41.149.84	8/icmp	1
36.2.39.81	8/icmp	1
39.118.46.88	8/icmp	1
42.116.199.113	8/icmp	1
44.127.157.74	8/icmp	1
50.150.192.35	8/icmp	1
52.133.60.60	8/icmp	1
79.35.88.10	8/icmp	1
81.211.52.112	8/icmp	1
97.18.48.18	8/icmp	1
103.101.163.14	8/icmp	1
110.106.152.121	8/icmp	1
119.234.47.21	8/icmp	1
125.251.225.110	8/icmp	1
133.27.216.40	8/icmp	1
140.6.24.65	8/icmp	1
155.18.92.0	8/icmp	1
191.123.13.120	8/icmp	1
192.168.17.21	33381/udp	2
207.220.12.1	8/icmp	1
226.141.148.115	8/icmp	1
236.191.169.26	8/icmp	1
237.143.1.120	8/icmp	1
242.67.108.105	8/icmp	1
IPs	**Resources**	**Connections**
25	2	26

Tabla 14 Resumen 5 de actividad identificada

INCIDENCIA NUM. 2 Honeypot: 192.168.17.150		
Source IP	Resource	Connections
169.254.90.77	137/udp	5
	3/icmp	1
	8/icmp	18
192.168.17.21	33381/udp	7
	8/icmp	4
192.168.17.68	8/icmp	4

IPs	Resources	Connections
3	4	39

Tabla 15 Resumen 6 de actividad identificada

Al analizar la información obtenida del sistema con la dirección 192.168.17.150 fue posible identificar la presencia de la dirección 192.168.17.21 que al igual que en las ocasiones anteriores también realizó conexiones al destino 33381/udp con 2 conexiones en la primera incidencia y 7 en la segunda; además de 4 conexiones más dirigidas al destino 8/icmp, el cual en esta ocasión también es el destino con mayor ocurrencia en ambas incidencias.

Es importante también mencionar la presencia de la dirección 192.168.17.68 que permite descartar las demás direcciones fuente ya que es una de las dos direcciones que se encuentran en el segmento utilizado; además de que se presentó en todas las incidencias de los tres sistemas simulados.

En la siguiente tabla se muestran las direcciones fuentes identificadas, así como el número de conexiones realizadas por cada IP.

INCIDENCIA NÚM. 1

Top 10 Source Hosts

Rank	Source IP	Connections
1	192.168.17.21	10
2	31.86.191.30	1
3	249.185.62.5	1
4	67.87.0.94	1
5	116.207.59.50	1
6	73.122.183.94	1
7	206.34.40.32	1
8	30.20.6.27	1
9	41.152.214.101	1
10	86.164.181.85	1

Tabla 16 Resumen 7 de actividad identificada

INCIDENCIA NUM. 2

Top 10 Source Hosts

Rank	Source IP	Connections
1	169.254.90.77	91
2	192.168.17.21	57
3	192.168.17.68	24

Tabla 17 Resumen 8 de actividad identificada

La tabla siguiente muestra de forma específica la cantidad de conexiones por puerto realizadas.

INCIDENCIA NUM. 1

Top 10 Accessed Resources

Rank	Resource	Connections
1	8/icmp	87
2	33381/udp	7
3	80/tcp	3

Tabla 18 Resumen 9 de actividad identificada

INCIDENCIA NUM. 2

Top 10 Accessed Resources

Rank	Resource	Connections
1	8/icmp	111
2	33381/udp	25
3	137/udp	25
4	3/icmp	8
5	80/tcp	3

Tabla 19 Resumen 10 de actividad identificada

La información siguiente específica la cantidad de conexiones realizadas por dirección identificada de forma general.

INCIDENCIA NUM. 1

Top 10 ICMP > 40 bytes Senders

Rango	Dirección fuente	Conexiones
1	31.86.191.30	1
2	249.185.62.5	1
3	67.87.0.94	1
4	116.207.59.50	1
5	73.122.183.94	1
6	206.34.40.32	1
7	30.20.6.27	1
8	41.152.214.101	1
9	86.164.181.85	1
10	37.54.134.7	1

Tabla 20 Resumen 11 de actividad identificada

INCIDENCIA NUM. 2 Top 10 ICMP > 40 bytes Senders		
Rango	**Dirección fuente**	**Conexiones**
1	169.254.90.77	66
2	192.168.17.21	29
3	192.168.17.68	24

Tabla 21 Resumen 12 de actividad identificada

Para finalizar con el reporte de los dos primeros ataques se muestran las conexiones realizadas por hora.

INCIDENCIA NUM. 1 Conexiones por hora	
Hora	**Conexiones**
00:00	0
01:00	0
02:00	0
03:00	0
-	-
-	-
18:00	0
19:00	97

Tabla 22 Resumen 13 de actividad identificada

INCIDENCIA NÚM. 2 Conexiones por hora	
00:00	0
01:00	0
02:00	0
03:00	0
-	-
-	-
21:00	14
22:00	124
23:00	34

Tabla 23 Resumen 14 de actividad identificada

Analizando la información de las tablas anteriores y tomando en cuenta los datos más relevante es posible deducir que el destino con mayor ocurrencia de conexiones fue 8/icmp teniendo en total 87 conexiones en la primera incidencia y 111 en la segunda, seguido por el puerto 33381/udp y 137/udp; como era de esperarse al dejar los sistemas con vulnerabilidades la cantidad de conexiones fue en aumento desde la primera fase de conexiones hasta la segunda, aparte no se refiere a un aumento gradual, ni dirigido a un puerto respectivamente, ni a una dirección en particular, al analizar el comportamiento y la cantidad de las conexiones realizadas y dirigidas a los sistemas que se encontraban con mayor vulnerabilidad, se esperaba que el sistema con la dirección 192.168.17.110 tuviera mayor cantidad de intrusiones, si lo que buscaba el atacante era sólo inhabilitar el sistema más expuesto sin tomar en cuenta la importancia de la información contenida o los servicios que provee; aparte no se simuló ningún servicio a diferencia de la configuración de los otros dos sistemas; ahora bien se denota que la cantidad de conexiones realizadas hacia los demás sistemas no es mucha; esto provee un gran avance ya que este comportamiento es predecible en un sistema que simplemente busca puertos abiertos realizando de esta forma una exploración de la red y recabar información de la misma.

Es posible deducir en primera instancia que las primeras 2 incidencias sólo se trataron de una exploración y la última un ataque de denegación de servicio realizado, además de que el autor de dicho ataque no estaba interesado en la información que contenían los sistemas a los cuales realizó el ataque, simplemente realizó el irrupción al sistema más vulnerable y así consiguió su cometido logrando la inhabilitación del servidor *Honeypot*.

CONCLUSIONES

Uno de los principales objetivos de implementar un Honeypot es disuadir al intruso en un eventual ataque para así comprometer el sistema Honeypot antes de permitir amenazas en los sistemas reales y además obtener evidencia digital de las condiciones en las que se perpetra un ataque.

Una vez comprometido el sistema se procedió a extraer los archivos de información que se generaron al momento del ataque, con los cuales fue posible determinar el tipo de ataque que se intentó realizar, así como también los puertos a los cuales fueron lanzados, la hora, cantidad y direcciones fuente de las cuales se detecto actividad mal intencionada hacia el sistema, esta información obtenida representa una ventaja ante los posibles nuevos ataques que su puedan realizar a los sistemas.

Para presentar un escenario falso a un intruso se trazó un plan debidamente, ya que en el desarrollo del proyecto se presentaron situaciones que por cuestiones de seguridad y credibilidad fue necesario utilizar otras herramientas que fortalezcan al Honeypot, dicho caso fue el de FARPD y NMAP, con estas herramientas fue posible validar los sistemas operativos simulados y asignar direcciones ip de tal forma que simularan una gran red en función.

No solo hay que presentar un buen escenario, también fue preciso brindar la seguridad necesaria al sistema para que no sea perpetrado con relativa facilidad, tomando los criterios de seguridad de sistemas, en este proyecto es necesario configurar por mínimo la seguridad básica para no ser descubierto con facilidad y hacer que nuestro intruso caiga en la trampa.

La configuración de cada sistema operativo es importante ya que es necesario presentar todos los elementos indispensables de una red real, con esto me refiero al sistema operativo que tendría cada equipo, cuáles puertos tendrían habilitados, cuáles puertos estarían bloqueados y cuáles darían respuesta de acuerdo al papel que tomarían en la escena, cabe mencionar que en la creación de los scrips es posible agregar otros que simulen diversos servicios, tales como, servidores web, proxy, e inclusive simular un router.

En el honeypot que se configuro se simuló un servidor web en el cual se dejaron abiertos los puertos tcp139, tcp137 y udp 137 ya que son los puertos más comunes en recibir intrusiones, además de esta vulnerabilidad también se agregó un scrip que simularía respuesta a conexiones telnet que después de unos segundos de recaudar información bloquearía los intentos de conexión; el resultado de esto fue exitoso ya que los puertos que se dejaron abiertos resultaron ser los que recibieron la mayor cantidad de intentos de conexión, cabe mencionar que el scrip del servicio de telnet agregado fue también considerado con el mayor rango de intentos de conexiones.

Como se menciona antes un servidor trampa es cuestión de organización y estrategia, ya que para entrar en escena es necesario presentar el sistema adecuado, con vulnerabilidades y a la vez con seguridad para no presentar sospechas.

Finalmente hay que destacar que todos los ataques fueron direccionados al servidor trampa y que el servidor real no fue detectado ni corrompido, esto indica que Honeypot es un agente distractor, que si es bien aprovechado debe tener muy buenos resultados en lo que respecta a la seguridad de sistemas de información.

BIBLIOGRAFÍA

Borghello, C. (2009). Amenazas Lógicas - Tipos de Ataques - Denial of Service (DoS). Recuperado el 03 de 2011, de http://www.segu-info.com.ar/ataques/ataques_dos.htm

Comunidad Ubuntu. (2011). "farpd" package in Ubuntu. Recuperado el 01 de 10 de 2010, de https://launchpad.net/ubuntu/+source/farpd

Honeynet.BR Project. (11 de Julio de 2008). *Honeynet.BR Project*. Recuperado el 11 de 2010, de http://www.honeynet.org.br/tools/

KAFSENSOR. (s.f.). Recuperado el febrero de 2011, de http://www.keyfocus.net/kfsensor/

Lyon, G. (1997). *NMAP.ORG*. Recuperado el 03 de 2011, de http://insecure.org

McAfee. (2003-2011). *Mcafee*. Recuperado el 03 de 2011, de http://www.mcafee.com/threat-intelligence/malware

McKennish, R. (1998). *Donald Mackay Churchill Fello ws hip to Study Overseas Developments in Forensic Computing.* Australia.

Óscar López, H. A. (2001). *INFORMÁTICA FORENSE : GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS.* Colombia.

Provos, N. (15 de Julio de 2008). *Developments of the Honeyd Virtual Honeypot* . Recuperado el 25 de 12 de 2010, de http://www.honeyd.org/index.php

Rivera, G. A. *Informática forense.* Universidad San Carlos de Guatemala.

Spitzner, L. (8 de Abril de 2003). Specter: a Commercial Honeypot Solution for Windows.

Wesley, A. (2002). *The Honeynet Project, Know Your Enemy. Revealing the security tools, tactics, and mo-tives of the blackhat community.* Boston.

WIKIPEDIA. (15 de MARZO de 2011). *WIKIPEDIA*. Recuperado el ABRIL de 2011, de http://es.wikipedia.org/wiki/Honeypot

Xubuntu, C. (2011). *http://www.xubuntu.org*. Recuperado el 02 de 2011, de http://www.xubuntu.org/about

Anexo A: INFORMACIÓN DE TERCERA INCIDENCIA

ANEXOS

INFORMACIÓN DE TERCERA INCIDENCIA

52615/tcp 1
52616/tcp 1
52617/tcp 1
52618/tcp 1
52619/tcp 1
52620/tcp 1
52621/tcp 1
52622/tcp 1
52623/tcp 1
52624/tcp 1
52625/tcp 1
52626/tcp 1
52627/tcp 1
52628/tcp 1
52629/tcp 1
52630/tcp 1
52631/tcp 1
52632/tcp 1
52633/tcp 1
52634/tcp 1
52635/tcp 1
52636/tcp 1
52637/tcp 1
52638/tcp 1
52639/tcp 1
52640/tcp 1
52641/tcp 1
52642/tcp 1
52643/tcp 1
52644/tcp 1
52645/tcp 1
52646/tcp 1
52647/tcp 1
52648/tcp 1
52649/tcp 1
52650/tcp 1
52651/tcp 1
52652/tcp 1
52653/tcp 1
52654/tcp 1
52655/tcp 1
52656/tcp 1

52657/tcp 1
52658/tcp 1
52659/tcp 1
52660/tcp 1
52661/tcp 1
52662/tcp 1
52663/tcp 1
52664/tcp 1
52665/tcp 1
52666/tcp 1
52667/tcp 1
52668/tcp 1
52669/tcp 1
52670/tcp 1
52671/tcp 1
52672/tcp 1
52673/tcp 1
52674/tcp 1
52675/tcp 1
52676/tcp 1
52677/tcp 1
52678/tcp 1
52679/tcp 1
52680/tcp 1
52681/tcp 1
52682/tcp 1
52683/tcp 1
52684/tcp 1
52685/tcp 1
52686/tcp 1
52687/tcp 1
52688/tcp 1
52689/tcp 1
52690/tcp 1
52691/tcp 1
52692/tcp 1
52693/tcp 1
52694/tcp 1
52695/tcp 1
52696/tcp 1
52697/tcp 1
52698/tcp 1
52699/tcp 1
52700/tcp 1
52701/tcp 1
52702/tcp 1
52703/tcp 1
52704/tcp 1
52705/tcp 1
52706/tcp 1

52707/tcp 1
52708/tcp 1
52709/tcp 1
52710/tcp 1
52711/tcp 1
52712/tcp 1
52713/tcp 1
52714/tcp 1
52715/tcp 1
52716/tcp 1
52717/tcp 1
52718/tcp 1
52719/tcp 1
52720/tcp 1
52721/tcp 1
52722/tcp 1
52723/tcp 1
52724/tcp 1
52725/tcp 1
52726/tcp 1
52727/tcp 1
52728/tcp 1
52729/tcp 1
52730/tcp 1
52731/tcp 1
52732/tcp 1
52733/tcp 1
52734/tcp 1
52735/tcp 1
52736/tcp 1
52737/tcp 1
52738/tcp 1
52739/tcp 1
52740/tcp 1
52741/tcp 1
52742/tcp 1
52743/tcp 1
52744/tcp 1
52745/tcp 1
52746/tcp 1
52747/tcp 1
52748/tcp 1
52749/tcp 1
52750/tcp 1
52751/tcp 1
52752/tcp 1
52753/tcp 1
52754/tcp 1
52755/tcp 1
52756/tcp 1

52757/tcp 1
52758/tcp 1
52759/tcp 1
52760/tcp 1
52761/tcp 1
52762/tcp 1
52763/tcp 1
52764/tcp 1
52765/tcp 1
52766/tcp 1
52767/tcp 1
52768/tcp 1
52769/tcp 1
52770/tcp 1
52771/tcp 1
52772/tcp 1
52773/tcp 1
52774/tcp 1
52775/tcp 1
52776/tcp 1
52777/tcp 1
52778/tcp 1
52779/tcp 1
52780/tcp 1
52781/tcp 1
52782/tcp 1
52783/tcp 1
52784/tcp 1
52785/tcp 1
52786/tcp 1
52787/tcp 1
52788/tcp 1
52789/tcp 1
52790/tcp 1
52791/tcp 1
52792/tcp 1
52793/tcp 1
52794/tcp 1
52795/tcp 1
52796/tcp 1
52797/tcp 1
52798/tcp 1
52799/tcp 1
52800/tcp 1
52801/tcp 1
52802/tcp 1
52803/tcp 1
52804/tcp 1
52805/tcp 1
52806/tcp 1

52807/tcp 1
52808/tcp 1
52809/tcp 1
52810/tcp 1
52811/tcp 1
52812/tcp 1
52813/tcp 1
52814/tcp 1
52815/tcp 1
52816/tcp 1
52817/tcp 1
52818/tcp 1
52819/tcp 1
52820/tcp 1
52821/tcp 1
52822/tcp 1
52823/tcp 1
52824/tcp 1
52825/tcp 1
52826/tcp 1
52827/tcp 1
52828/tcp 1
52829/tcp 1
52830/tcp 1
52831/tcp 1
52832/tcp 1
52833/tcp 1
52834/tcp 1
52835/tcp 1
52836/tcp 1
52837/tcp 1
52838/tcp 1
52839/tcp 1
52840/tcp 1
52841/tcp 1
52842/tcp 1
52843/tcp 1
52844/tcp 1
52845/tcp 1
52846/tcp 1
52847/tcp 1
52848/tcp 1
52849/tcp 1
52850/tcp 1
52851/tcp 1
52852/tcp 1
52853/tcp 1
52854/tcp 1
52855/tcp 1
52856/tcp 1

52857/tcp 1
52858/tcp 1
52859/tcp 1
52860/tcp 1
52861/tcp 1
52862/tcp 1
52863/tcp 1
52864/tcp 1
52865/tcp 1
52866/tcp 1
52867/tcp 1
52868/tcp 1
52869/tcp 1
52870/tcp 1
52871/tcp 1
52872/tcp 1
52873/tcp 1
52874/tcp 1
52875/tcp 1
52876/tcp 1
52877/tcp 1
52878/tcp 1
52879/tcp 1
52880/tcp 1
52881/tcp 1
52882/tcp 1
52883/tcp 1
52884/tcp 1
52885/tcp 1
52886/tcp 1
52887/tcp 1
52888/tcp 1
52889/tcp 1
52890/tcp 1
52891/tcp 1
52892/tcp 1
52893/tcp 1
52894/tcp 1
52895/tcp 1
52896/tcp 1
52897/tcp 1
52898/tcp 1
52899/tcp 1
52900/tcp 1
52901/tcp 1
52902/tcp 1
52903/tcp 1
52904/tcp 1
52905/tcp 1
52906/tcp 1

52907/tcp 1
52908/tcp 1
52909/tcp 1
52910/tcp 1
52911/tcp 1
52912/tcp 1
52913/tcp 1
52914/tcp 1
52915/tcp 1
52916/tcp 1
52917/tcp 1
52918/tcp 1
52919/tcp 1
52920/tcp 1
52921/tcp 1
52922/tcp 1
52923/tcp 1
52924/tcp 1
52925/tcp 1
52926/tcp 1
52927/tcp 1
52928/tcp 1
52929/tcp 1
52930/tcp 1
52931/tcp 1
52932/tcp 1
52933/tcp 1
52934/tcp 1
52935/tcp 1
52936/tcp 1
52937/tcp 1
52938/tcp 1
52939/tcp 1
52940/tcp 1
52941/tcp 1
52942/tcp 1
52943/tcp 1
52944/tcp 1
52945/tcp 1
52946/tcp 1
52947/tcp 1
52948/tcp 1
52949/tcp 1
52950/tcp 1
52951/tcp 1
52952/tcp 1
52953/tcp 1
52954/tcp 1
52955/tcp 1
52956/tcp 1

52957/tcp 1
52958/tcp 1
52959/tcp 1
52960/tcp 1
52961/tcp 1
52962/tcp 1
52963/tcp 1
52964/tcp 1
52965/tcp 1
52966/tcp 1
52967/tcp 1
52968/tcp 1
52969/tcp 1
52970/tcp 1
52971/tcp 1
52972/tcp 1
52973/tcp 1
52974/tcp 1
52975/tcp 1
52976/tcp 1
52977/tcp 1
52978/tcp 1
52979/tcp 1
52980/tcp 1
52981/tcp 1
52982/tcp 1
52983/tcp 1
52984/tcp 1
52985/tcp 1
52986/tcp 1
52987/tcp 1
52988/tcp 1
52989/tcp 1
52990/tcp 1
52991/tcp 1
52992/tcp 1
52993/tcp 1
52994/tcp 1
52995/tcp 1
52996/tcp 1
52997/tcp 1
52998/tcp 1
52999/tcp 1
53000/tcp 1
53001/tcp 3
53002/tcp 1
53003/tcp 1
53004/tcp 1
53005/tcp 1
53006/tcp 1

53007/tcp 1
53008/tcp 1
53009/tcp 1
53010/tcp 1
53011/tcp 1
53012/tcp 1
53013/tcp 1
53014/tcp 1
53015/tcp 1
53016/tcp 1
53017/tcp 1
53018/tcp 1
53019/tcp 1
53020/tcp 1
53021/tcp 1
53022/tcp 1
53023/tcp 1
53024/tcp 1
53025/tcp 1
53026/tcp 1
53027/tcp 1
53028/tcp 1
53029/tcp 1
53030/tcp 1
53031/tcp 1
53032/tcp 1
53033/tcp 1
53034/tcp 1
53035/tcp 1
53036/tcp 1
53037/tcp 1
53038/tcp 1
53039/tcp 1
53040/tcp 1
53041/tcp 1
53042/tcp 1
53043/tcp 1
53044/tcp 1
53045/tcp 1
53046/tcp 1
53047/tcp 1
53048/tcp 1
53049/tcp 1
53050/tcp 1
53051/tcp 1
53052/tcp 1
53053/tcp 1
53054/tcp 1
53055/tcp 1
53056/tcp 1

53057/tcp 1
53058/tcp 1
53059/tcp 1
53060/tcp 1
53061/tcp 1
53062/tcp 1
53063/tcp 1
53064/tcp 1
53065/tcp 1
53066/tcp 1
53067/tcp 1
53068/tcp 1
53069/tcp 1
53070/tcp 1
53071/tcp 1
53072/tcp 1
53073/tcp 1
53074/tcp 1
53075/tcp 1
53076/tcp 1
53077/tcp 1
53078/tcp 1
53079/tcp 1
53080/tcp 1
53081/tcp 1
53082/tcp 1
53083/tcp 1
53084/tcp 1
53085/tcp 1
53086/tcp 1
53087/tcp 1
53088/tcp 1
53089/tcp 1
53090/tcp 1
53091/tcp 1
53092/tcp 1
53093/tcp 1
53094/tcp 1
53095/tcp 1
53096/tcp 1
53097/tcp 1
53098/tcp 1
53099/tcp 1
53100/tcp 1
53101/tcp 1
53102/tcp 1
53103/tcp 1
53104/tcp 1
53105/tcp 1
53106/tcp 1

53107/tcp 1
53108/tcp 1
53109/tcp 1
53110/tcp 1
53111/tcp 1
53112/tcp 1
53113/tcp 1
53114/tcp 1
53115/tcp 1
53116/tcp 1
53117/tcp 1
53118/tcp 1
53119/tcp 1
53120/tcp 1
53121/tcp 1
53122/tcp 1
53123/tcp 1
53124/tcp 1
53125/tcp 1
53126/tcp 1
53127/tcp 1
53128/tcp 1
53129/tcp 1
53130/tcp 1
53131/tcp 1
53132/tcp 1
53133/tcp 1
53134/tcp 1
53135/tcp 1
53136/tcp 1
53137/tcp 1
53138/tcp 1
53139/tcp 1
53140/tcp 1
53141/tcp 1
53142/tcp 1
53143/tcp 1
53144/tcp 1
53145/tcp 1
53146/tcp 1
53147/tcp 1
53148/tcp 1
53149/tcp 1
53150/tcp 1
53151/tcp 1
53152/tcp 1
53153/tcp 1
53154/tcp 1
53155/tcp 1
53156/tcp 1

53157/tcp 1
53158/tcp 1
53159/tcp 1
53160/tcp 1
53161/tcp 1
53162/tcp 1
53163/tcp 1
53164/tcp 1
53165/tcp 1
53166/tcp 1
53167/tcp 1
53168/tcp 1
53169/tcp 1
53170/tcp 1
53171/tcp 1
53172/tcp 1
53173/tcp 1
53174/tcp 1
53175/tcp 1
53176/tcp 1
53177/tcp 1
53178/tcp 1
53179/tcp 1
53180/tcp 1
53181/tcp 1
53182/tcp 1
53183/tcp 1
53184/tcp 1
53185/tcp 1
53186/tcp 1
53187/tcp 1
53188/tcp 1
53189/tcp 1
53190/tcp 1
53191/tcp 1
53192/tcp 1
53193/tcp 1
53194/tcp 1
53195/tcp 1
53196/tcp 1
53197/tcp 1
53198/tcp 1
53199/tcp 1
53200/tcp 1
53201/tcp 1
53202/tcp 1
53203/tcp 1
53204/tcp 1
53205/tcp 1
53206/tcp 1

53207/tcp 1
53208/tcp 1
53209/tcp 1
53210/tcp 1
53211/tcp 1
53212/tcp 1
53213/tcp 1
53214/tcp 1
54320/tcp 2
54321/tcp 2
54345/tcp 2
55301/tcp 1
57341/tcp 2
59595/tcp 2
60008/tcp 2
60177/tcp 2
60179/tcp 2
61439/tcp 2
61440/tcp 2
61441/tcp 2
61446/tcp 2
65000/tcp 2
65001/tcp 1
65301/tcp 2
65432/tcp 1
65534/tcp 2
8/icmp 5
13/icmp 2
15/icmp 3
17/icmp 4
37/icmp 1

IPs Recursos Conexiones
2 53233 62664

Anexo B:

INSTALAR UN SERVIDOR WEB Y DE CORREO CONFIGURADO CON ISPCONFIG.

INSTALAR UN SERVIDOR WEB Y DE CORREO CONFIGURADO CON ISPCONFIG.

AJUSTAR /ETC/HOSTS

El primer paso es realizar los ajustes necesarios en el archivo /etc/hosts como se muestra a continuación:

vi /etc/hosts

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1    localhost.localdomain localhost
192.168.1.38   proyecto2.honey.com server1
::1    localhost6.localdomain6 localhost6
```

Activar el Firewall y SELinux

SELinux es una extensión de CentOS que puede brindar una mayor seguridad, para activarlo son necesarios los siguientes comandos:

Se selecciona SELinux para deshabilitarlo, aplicar y aceptar.

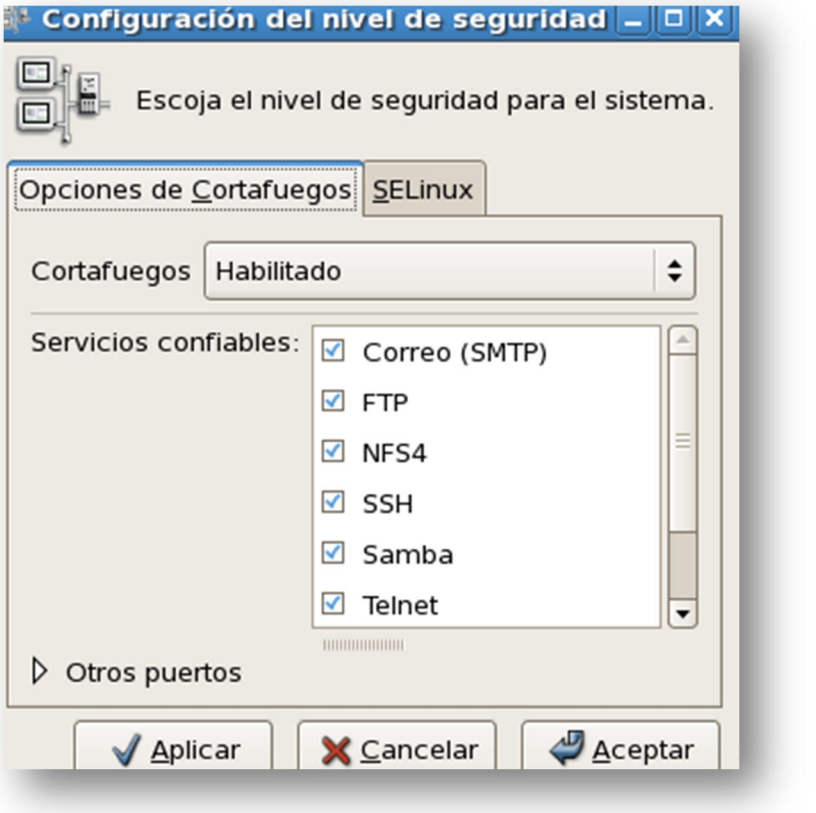

Fig. 7 Configuración del nivel de seguridad

A continuación se reinicia el sistema

Reboot

Instalar pre requisitos.

Primero se importa las llaves GPG para los paquetes que se utilizarán:

*rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY**

Después se actualizan los paquetes existentes en el sistema:

yum update

Ahora se instalan los paquetes de software que se necesitaran después:

yum install fetchmail wget bzip2 unzip zip nmap openssl lynx fileutils ncftp gcc gcc-c++

Instalar Cuota

Se instala la cuota con el siguiente comando:

yum install quota

Se edita el archivo /etc/fstab y se añade, usrquota,grpquota a la partición (/dev/VolGroup00/LogVol00):

```
nano /etc/fstab
/dev/VolGroup00/LogVol00 / ext3 defaults,usrquota,grpquota          1 1
LABEL=/boot /boot  ext3  defaults                        1 2
tmpfs   /dev/shm tmpfs  defaults              0 0
devpts   /dev/pts devpts  gid=5,mode=620          0 0
sysfs   /sys  sysfs  defaults                    0 0
proc   /proc  proc  defaults                    0 0
/dev/VolGroup00/LogVol01 swap swap defaults                0 0
```

Para habilitar la cuota se ejecuta

touch /aquota.user /aquota.group
*chmod 600 /aquota.**
mount -o remount /
quotacheck -avugm
quotaon –avug

INSTALAR APACHE, MySQL y phpMyAdmin

Primero se habilitan los repositorios RPMforge en el sistema CentOS ya que muchos de los paquetes que se utilizaran no están disponibles en los repositorios de CentOS.

rpm --import http://dag.wieers.com/rpm/packages/RPM-GPG-KEY.dag.txt
cd /tmp
wget http://dag.wieers.com/rpm/packages/rpmforge-release/rpmforge-release-

0.3.6-1.el5.rf.x86_64.rpm
rpm -ivh rpmforge-release-0.3.6-1.el5.rf.x86_64.rpm

Ahora es posible instalar los paquetes necesarios con la siguiente línea:

yum install ntp httpd mysql-server php php-mysql php-mbstring php-mcrypt phpmyadmin rpm-build gcc mysql-devel openssl-devel cyrus-sasl-devel pkgconfig zlib-devel pcre-devel openldap-devel postgresql-devel expect libtool-ltdl-devel openldap-servers libtool gdbm-devel pam-devel

Instalar Courier-IMAP, Courier-Authlib y Maildrop

Desafortunadamente no hay paquetes rpm para Courier-IMAP, Courier authlib-, y maildrop, por lo que es necesario construirlos.

Los paquetes RPM no deben construirse como root, courier-imap incluso se negará a compilar si detecta que la compilación se ejecuta como el usuario root. Por lo que se crea una cuenta de usuario normal ahora (compileuser en este ejemplo) y se asigna una contraseña:
useradd -m -s /bin/bash compileuser
passwd compileuser

El comando sudo es necesario para que el usuario compileuser pueda compilar e instalar los paquetes rpm. Por lo que se debe permitir que compileuser para ejecutar todos los comandos con sudo:

Ejecutar:

Visudo

En el archivo que se abre hay una línea de root ALL = (ALL) ALL se agrega una línea similar para compileuser justo debajo de esa línea:

```
[...]
root ALL=(ALL)  ALL
compileuser ALL=(ALL)  ALL
[...]
```

Ahora todo está listo para construir los paquetes rpm el primer paso es identificarse como el usuario compileuser:

su compileuser

Se crean los directorios para compilar

mkdir $ HOME / rpm

mkdir $ HOME / rpm / SOURCES

mkdir $ HOME / rpm / SPECS

mkdir $ HOME / rpm / BUILD

mkdir $ HOME / rpm / SRPMS

mkdir $ HOME / rpm / RPMS

$ mkdir HOME/rpm/RPMS/i386

$ mkdir HOME/rpm/RPMS/x86_64

echo "_topdir% $ HOME / rpm">> $ HOME / .rpmmacros

Se descargan los archivos fuente de la página http://www.courier-mta.org/download.php:

cd /tmp
wget http://prdownloads.sourceforge.net/courier/courier-authlib-0.62.4.tar.bz2
wget http://prdownloads.sourceforge.net/courier/courier-imap-4.6.0.tar.bz2
wget http://prdownloads.sourceforge.net/courier/maildrop-2.2.0.tar.bz2

Ahora es posible construir courier-authlib con el siguiente comando:

sudo rpm-ivh maildrop-2.2.0-1.x86_64.rpm

Los paquetes rpm se pueden encontrar en $ HOME/rpm/RPMS/x86_64.

cd $ HOME/rpm/RPMS/x86_64

Con el comando ls –l se listan los paquetes disponibles

[Compileuser @ servidor1 x86_64] $ ls-l
total de 676
-Rw-r - r - 1 root raíz 153870 28 de octubre 15:39 courier-authlib-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 385183 28 de octubre 15:39 courier-authlib-debuginfo-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 36260 28 de octubre 15:39 courier-authlib-devel-0.62.4-1.x86_64.rpm

-Rw-r - r - 1 root root 18434 28 de octubre 15:39 courier-authlib-ldap-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 14617 28 de octubre 15:39 courier-authlib-mysql-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 13826 28 de octubre 15:39 courier-authlib-pgsql-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 28 de octubre 8484 15:39 courier-authlib-pipe-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 35388 28 de octubre 15:39 courier-authlib-userdb-0.62.4-1.x86_64.rpm
[Compileuser @ servidor1 x86_64] $

Se instalan los paquetes necesarios

sudo rpm-ivh courier-authlib-0.62.4-1.x86_64.rpm mensajería courier-authlib-mysql-0.62.4-1.x86_64.rpm-authlib-devel-0.62.4-1.x86_64.rpm

Ahora volvemos al directorio /tmp y se ejecuta rpmbuild de nuevo, esta vez sin sudo, de lo contrario la compilación fallará porque se ejecute como root:
cd / tmp
rpmbuild-ta courier-imap-4.6.0.tar.bz2

una vez finalizado el proceso los paquetes rpm se pueden encontrar en $ HOME/rpm/RPMS/x86_64
cd $ HOME/rpm/RPMS/x86_64

El comando ls -l muestra los paquetes rpm disponibles:
[Compileuser @ servidor1 x86_64] $ ls-l
total de 1996
-Rw-r - r - 1 root root 153870 28 de octubre 15:39 courier-authlib-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root raíz 385183 28 de octubre 15:39 courier-authlib-debuginfo-0.62.4 1.x86_64.rpm-
-Rw-r - r - 1 root root 36260 28 de octubre 15:39 courier-authlib-devel-0.62.4-1.x86_64.rpm
, Rw-r - r - 1 root root 18434 28 de octubre 15:39 courier-authlib, ldap-0.62.4, 1.x86_64.rpm
-Rw-r - r - 1 root root 14617 28 de octubre 15:39 courier-authlib-mysql-0.62.4-1.x86_64.rpm

-Rw-r - r - 1 root root 13826 28 de octubre 15:39 courier-authlib-pgsql-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 28 de octubre 8484 15:39 courier-authlib-pipe-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 35388 28 de octubre 15:39 courier-authlib-userdb-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 compileuser compileuser 400497 28 de octubre 15:49 courier-imap-4.6.0-1.x86_64.rpm
-Rw-r - r - 1 compileuser compileuser 941203 28 de octubre 15:49 courier-imap-4.6.0-debuginfo-1.x86_64.rpm
[Compileuser @ servidor1 x86_64] $

Puede instalar courier-imap con el siguiente comando:
sudo rpm-ivh courier-imap-4.6.0-1.x86_64.rpm

Es preciso regresar a /tmp y ejecutar rpmbuild nuevo, esta vez para construir el paquete maildrop:
cd / tmp
sudo rpmbuild-ta-maildrop 2.2.0.tar.bz2

Los paquetes rpm se pueden encontrar en $ HOME/rpm/RPMS/x86_64

cd $ HOME/rpm/RPMS/x86_64

El comando ls -l muestra los paquetes rpm disponibles:
[Compileuser @ servidor1 x86_64] $ ls-l
total de 3256
-Rw-r - r - 1 root root 153870 28 de octubre 15:39 courier-authlib-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 385183 28 de octubre 15:39 courier-authlib-debuginfo-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 36260 28 de octubre 15:39 courier-authlib-devel-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 18434 28 de octubre 15:39 courier-authlib-ldap-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 14617 28 de octubre 15:39 courier-authlib-mysql-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 13826 28 de octubre 15:39 courier-authlib-pgsql-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 28 de octubre 8484 15:39 courier-authlib-pipe-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 root root 35388 28 de octubre 15:39 courier-authlib-userdb-0.62.4-1.x86_64.rpm
-Rw-r - r - 1 compileuser compileuser 400497 28 de octubre 15:49 courier-imap-4.6.0-1.x86_64.rpm
-Rw-r - r - 1 compileuser compileuser 941203 28 de octubre 15:49 courier-imap-

4.6.0-debuginfo-1.x86_64.rpm
-Rw-r - r - 1 root root 299284 28 de octubre 15:55 maildrop-2.2.0-1.x86_64.rpm
-Rw-r - r - 1 root root 769256 28 de octubre 15:55 maildrop-2.2.0-debuginfo-1.x86_64.rpm
-Rw-r - r - 1 root root 134573 28 de octubre 15:55 maildrop-devel-2.2.0-1.x86_64.rpm
-Rw-r - r - 1 root root 63936 28 de octubre 15:55 maildrop-man-2.2.0-1.x86_64.rpm
[Compileuser @ servidor1 x86_64] $

Ahora es posible instalar maildrop:
sudo rpm-ivh maildrop-2.2.0-1.x86_64.rpm

Después de haber compilado e instalado todos los paquetes necesarios, es posible regresar como root.

exit

Aplicar parche para cuota de Postfix

Se obtener el código fuente rpm de Postfix, el parche de la cuota y construir un nuevo paquete de Postfix rpm e instalarlo.
cd / usr / src
http://ftp-stud.fht-esslingen.de/pub/Mirrors/centos/5.4/os/SRPMS/postfix-2.3.3-2.1.el5_2.src.rpm wget
rpm-ivh postfix-2.3.3-2.1.el5_2.src.rpm

El último comando mostrará algunas advertencias de que puede pasar por alto:
warning: user mockbuild does not exist - using root
warning: group mockbuild does not exist - using root

cd / usr / src / redhat / SOURCES
wget http://vda.sourceforge.net/VDA/postfix-2.3.3-vda.patch.gz
gunzip postfix-2.3.3-vda.patch.gz
cd / usr / src / redhat / SPECS /

Editar el archivo postfix.spec:
nano postfix.spec

En este archivo es necesario cambiar la línea *%define MYSQL 0* por *%define MYSQL% 1*, agregar *Patch0: postfix-2.3.3-vda.patch* a la estrofa *# parches*, y por último añadir *% patch0-p1-b. Vda* a la estrofa *% setup-q:* como se muestra en el siguiente ejemplo:

[...]
1% definir MYSQL
[...]
Parches

Patch0: postfix-2.3.3-vda.patch
Patch1: postfix-2.1.1-config.patch
Patch3: postfix-alternatives.patch
Patch6: postfix-2.1.1-obsolete.patch
Patch7: postfix-2.1.5-aliases.patch
Patch8: postfix-gran fs.patch
Patch9: postfix-2.2.5-cyrus.patch
Patch10: postfix-CVE-2008-2936.patch
[...]
% Setup-q
# Aplicar parches obligatoria
% Patch0-p1-b. Vda
% Patch1-p1-b. Config
alternativas% patch3-p1-b.
% Patch6-p1-b. Obsoletos
alias% patch7-p1-b.
% Patch8-p1-b. Gran fs
% Patch9-p1-b. Cyrus
% Patch10-p1-b. CVE-2008-2.936
[...]

A partir de ahí el paquete rpm Postfix tiene cuotas y soporte de MySQL:
rpmbuild-ba postfix.spec

El paquete rpm Postfix se crea en / usr/src/redhat/RPMS/x86_64:
cd / usr/src/redhat/RPMS/x86_64

El comando ls -l muestra los paquetes disponibles:

[root @ servidor1 x86_64] # ls-l

total de 11732

-Rw-r - r - 1 root root 3940050 28 de octubre 16:02 postfix-2.3.3-2.1.x86_64.rpm

-Rw-r - r - 1 root root 7999345 28 de octubre 16:02 postfix-2.3.3-debuginfo-2.1.x86_64.rpm

-Rw-r - r - 1 root root 49759 28 de octubre 16:02 postfix-2.3.3-Pflogsumm-2.1.x86_64.rpm

[root @ servidor1 x86_64] #

Se elige el paquete postfix y se instala

rpm-ivh postfix-2.3.3-2.1.x86_64.rpm

A continuación, es necesario apagar Sendmail e iniciar Postfix, saslauthd y courier-authlib:

chkconfig --levels 235 courier-authlib on

/etc/init.d/courier-authlib start

chkconfig --levels 235 sendmail off

chkconfig --levels 235 postfix on

chkconfig --levels 235 saslauthd on

/etc/init.d/sendmail stop

/etc/init.d/postfix start

/etc/init.d/saslauthd start

Configurar Courier

El primer paso es crear los enlaces de inicio del sistema para courier-imap:

chkconfig --levels 235 courier-imap on

/etc/init.d/courier-authlib restart

/etc/init.d/courier-imap restart

Cuando courier-imap que se inicia por primera vez, crea automáticamente los archivos de certificados /usr/lib/courier-imap/share/imapd.pem y /usr/lib/courier-imap/share/pop3d.pem desde el directorio /usr/lib/courier-imap/etc/imapd.cnf/ y los archivos /usr/lib/courier-imap/etc/pop3d.cnf. Dado que los archivos cnf contienen la línea de CN = localhost, pero nuestro servidor se denomina proyecto2.honey.com, los certificados puede causar problemas cuando se utiliza conexiones TLS. Para solucionar esto, se borran ambos certificados.

cd /usr/lib/courier-imap/share/

rm -f imapd.pem

rm -f pop3d.pem

Reemplazar el CN = localhost en las líneas /usr/lib/courier-imap/etc/imapd.cnf y /usr/lib/courier-imap/etc/pop3d.cnf con CN = proyecto2.honey.com:

```
nano /usr/lib/courier-imap/etc/imapd.cnf
[...]
CN=proyecto2.honey.com
[...]
```

```
nano /usr/lib/courier-imap/etc/pop3d.cnf
[...]
CN=proyecto2.honey.com
[...]
```

En este momento se crean ambos certificados:

./mkimapdcert

./mkpop3dcert

Y se reinicia courier-authlib y courier-imap:

/etc/init.d/courier-authlib restart

/etc/init.d/courier-imap restart

Instalar Getmail

Getmail puede instalarse de la siguiente forma:

yum install getmail

Establecer passwords a MySQL y configurar phpMyAdmin

Iniciar MySQL:

chkconfig --levels 235 mysqld on

/etc/init.d/mysqld start

Establecer password a MySQL con la cuenta de root:

mysqladmin -u root password yourrootsqlpassword

mysqladmin -h proyecto2.honey.com -u root password yourrootsqlpassword

Configurar phpMyAdmin. Se cambia la configuración de Apache para que la conexión de phpMyAdmin no sea a través de localhost.

nano /etc/httpd/conf.d/phpmyadmin.conf

```
#
```

```
# Web application to manage MySQL
#

#<Directory "/usr/share/phpmyadmin">
# Order Deny,Allow
# Deny from all
# Allow from 127.0.0.1
#</Directory>

Alias /phpmyadmin /usr/share/phpmyadmin
Alias /phpMyAdmin /usr/share/phpmyadmin
Alias /mysqladmin /usr/share/phpmyadmin
```

Ahora se cambia la autenticación en phpMyAdmin de cookie a http:

nano /usr/share/phpmyadmin/config.inc.php

```
[...]
/* Authentication type */
$cfg['Servers'][$i]['auth_type'] = 'http';
[...]
```

El paso final es crear los enlaces de inicio del sistema para Apache e iniciar el servicio:

chkconfig --levels 235 httpd on

/etc/init.d/httpd start

Con esto es posible direccionar el navegador a http://proyecto2.honey.com/phpmyadmin/ o http://192.168.1.38/phpmyadmin/ e iniciar sesión con el usuario root y el nuevo password establecido.

Instalar Amavisd-new, SpamAssassin y ClamAV

Con ayuda del *yum* se instalan los servicios de Amavisd-new, SpamAssassin y ClamAV

yum install amavisd-new spamassassin clamav clamd unzip bzip2 unrar perl-DBD-mysql

Se inicia freshclam, amavisd, and clamd...

chkconfig --levels 235 amavisd on

chkconfig --levels 235 clamd on

/usr/bin/freshclam

/etc/init.d/amavisd start

/etc/init.d/clamd start

Se crean los directorios necesarios:

mkdir /var/run/amavisd /var/spool/amavisd /var/spool/amavisd/tmp /var/spool/amavisd/db

chown amavis /var/run/amavisd /var/spool/amavisd /var/spool/amavisd/tmp /var/spool/amavisd/db

Instalar Apache2 con mod_php, mod_fcgi/PHP5, y suPHP

mod_fcgid no es compatible con los repositorios de CentOS, pero son paquetes para CentOS 5.x en la página centos.karan.org es posible encontrar repositorios de prueba y se habilitan de la siguiente forma:

cd /etc/yum.repos.d/

wget http://centos.karan.org/kbsingh-CentOS-Extras.repo

Es preciso abrir el archivo /etc/yum.repos.d/kbsingh-CentOS-Extras.repo y establecer gpgcheck a 0 y enabled a 1 en la sección [kbs-CentOS-Testing]:

```
[...]
[kbs-CentOS-Testing]
name=CentOS.Karan.Org-EL$releasever - Testing
```

```
gpgcheck=0
gpgkey=http://centos.karan.org/RPM-GPG-KEY-karan.org.txt
enabled=1
baseurl=http://centos.karan.org/el$releasever/extras/testing/$basearch/RPMS/
```

Ahora es posible instalar Apache2 con mod_php5, mod_fcgid, y PHP5:

yum install php php-devel php-gd php-imap php-ldap php-mysql php-odbc php-pear php-xml php-xmlrpc php-eaccelerator php-mbstring php-mcrypt php-mhash php-mssql php-snmp php-soap php-tidy curl curl-devel perl-libwww-perl ImageMagick libxml2 libxml2-devel mod_fcgid php-cli httpd-devel

Se edita el archivo /etc/php.ini para cambiar el reporte de error añadiendo cgi.fix_pathinfo = 1 al final del archivo:

nano /etc/php.ini

```
[...]
;error_reporting = E_ALL
error_reporting = E_ALL & ~E_NOTICE
[...]
cgi.fix_pathinfo = 1
```

Para instalar suPHP se introducen los siguientes comandos:

cd /tmp

wget http://suphp.org/download/suphp-0.7.1.tar.gz

tar xvfz suphp-0.7.1.tar.gz

cd suphp-0.7.1/

./configure --prefix=/usr --sysconfdir=/etc --with-apr=/usr/bin/apr-1-config --with-apxs=/usr/sbin/apxs --with-apache-user=apache --with-setid-mode=owner --with-php=/usr/bin/php-cgi --with-logfile=/var/log/httpd/suphp_log --enable-SUPHP_USE_USERGROUP=yes

make

make install

Se añade el modulo de suPHP a la configuración de Apache.

nano /etc/httpd/conf.d/suphp.conf

LoadModule suphp_module modules/mod_suphp.so

Para finalizar se crea el archivo /etc/suphp.conf y se reinicia el servicio de Apache:

nano /etc/suphp.conf

```
[global]
;Path to logfile
logfile=/var/log/httpd/suphp.log

;Loglevel
loglevel=info

;User Apache is running as
webserver_user=apache

;Path all scripts have to be in
docroot=/

;Path to chroot() to before executing script
;chroot=/mychroot

; Security options
allow_file_group_writeable=true
allow_file_others_writeable=false
allow_directory_group_writeable=true
allow_directory_others_writeable=false

;Check wheter script is within DOCUMENT_ROOT
check_vhost_docroot=true

;Send minor error messages to browser
errors_to_browser=false
```

```
;PATH environment variable
env_path=/bin:/usr/bin

;Umask to set, specify in octal notation
umask=0077

; Minimum UID
min_uid=100

; Minimum GID
min_gid=100

[handlers]
;Handler for php-scripts
x-httpd-suphp="php:/usr/bin/php-cgi"

;Handler for CGI-scripts
x-suphp-cgi="execute:!self"
```

Reiniciar apache:

/etc/init.d/httpd restart

Instalar Vlogger y Webalizer

Vlogger y webalizer se instalan de la siguiente forma:

yum install webalizer perl-DateTime-Format-HTTP perl-DateTime-Format-Builder

cd /tmp

wget http://n0rp.chemlab.org/vlogger/vlogger-1.3.tar.gz

tar xvfz vlogger-1.3.tar.gz

mv vlogger-1.3/vlogger /usr/sbin/

*rm -rf vlogger**

Instalar fail2ban

Este paquete es recommendable instalarlo para ISPConfig:

yum install fail2ban

chkconfig --levels 235 fail2ban on

/etc/init.d/fail2ban start

Instalar rkhunter

rkhunter se instala con la siguiente línea de comandos:

yum install rkhunter

Instalar SquirrelMail

Para instalar el cliente de correo SquirrelMail se utilizan los siguientes comandos:

yum install squirrelmail

Y reiniciar el servicio de Apache:

/etc/init.d/httpd restart

Configurar Squirrelmail:

/usr/share/squirrelmail/config/conf.pl

Es necesario indicar a SquirrelMail que se utiliza Courier-IMAP/-POP3:

Squirrelmail Configuration : Read: config.php (1.4.0)

Main Menu --

1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

C Turn color off

S Save data

Q

Quit

Command >> <-- D

Squirrelmail Configuration : Read: config.php

While we have been building SquirrelMail, we have discovered some preferences that work better with some servers that don't work so well with others.

If you select your IMAP server, this option will
set some pre-defined settings for that server.

Please note that you will still need to go through and make sure
everything is correct. This does not change everything. There are
only a few settings that this will change.

Please select your IMAP server:
bincimap = Binc IMAP server
courier = Courier IMAP server
cyrus = Cyrus IMAP server
dovecot = Dovecot Secure IMAP server
exchange = Microsoft Exchange IMAP server
hmailserver = hMailServer
macosx = Mac OS X Mailserver
mercury32 = Mercury/32
uw = University of Washington's IMAP server

quit = Do not change anything
Command >> <-- courier

SquirrelMail Configuration : Read: config.php

While we have been building SquirrelMail, we have discovered some
preferences that work better with some servers that don't work so
well with others. If you select your IMAP server, this option will
set some pre-defined settings for that server.

Please note that you will still need to go through and make sure
everything is correct. This does not change everything. There are

only a few settings that this will change.

Please select your IMAP server:
bincimap = Binc IMAP server
courier = Courier IMAP server
cyrus = Cyrus IMAP server
dovecot = Dovecot Secure IMAP server
exchange = Microsoft Exchange IMAP server
hmailserver = hMailServer
macosx = Mac OS X Mailserver
mercury32 = Mercury/32
uw = University of Washington's IMAP server

quit = Do not change anything
Comando >> courier
imap_server_type = courier
default_folder_prefix = INBOX.
trash_folder = Trash
sent_folder = Sent
draft_folder = Drafts
show_prefix_option = false
default_sub_of_inbox = false
show_contain_subfolders_option = false
optional_delimiter = .
delete_folder = true

Press any key to continue... <-- presiona una tecla

SquirrelMail Configuration : Read: config.php (1.4.0)

Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)
8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

C Turn color off
S Save data
Q Quit

Comando >> <--S

SquirrelMail Configuration : Read: config.php (1.4.0)

Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books
7. Message of the Day (MOTD)

8. Plugins
9. Database
10. Languages

D. Set pre-defined settings for specific IMAP servers

C Turn color off
S Save data
Q Quit

Comando >> <--Q

El último archivo por modificar es /etc/squirrelmail/config_local.php en el cual se comenta la salida de la variable /etc/squirrelmail/config_local.php.

nano /etc/squirrelmail/config_local.php

```
<?php
/**
 * Local config overrides.
 *
 * You can override the config.php settings here.
 * Don't do it unless you know what you're doing.
 * Use standard PHP syntax, see config.php for examples.
 *
 * @copyright &copy; 2002-2006 The SquirrelMail Project Team
 * @license http://opensource.org/licenses/gpl-license.php GNU Public License
 * @version $Id: config_local.php,v 1.2 2006/07/11 03:33:47 wtogami Exp $
 * @package squirrelmail
 * @subpackage config
 */
//$default_folder_prefix    = '';
?>
```

Si no se hace esto es posible que al iniciar sesión en SquirrelMail se presente el siguiente error:

Query: CREATE "Sent" Reason Given: Invalid mailbox name.

Ahora es posible direccionar el navegador a http://proyecto2.honey.com/webmail o http://192.168.1.138/webmail y accesar a SquirrelMail.

Instalar SPConfig

Es preciso desinstalar BIND y Dovecot para que el instalador de ISPConfig configure ISPConfig para MyDNS y Courier:

yum remove bind dovecot

Se instala la última versión de ISPConfig con la siguiente línea de comandos:

cd /tmp

wget http://downloads.sourceforge.net/ispconfig/ISPConfig-3.0.1.6.tar.gz?use_mirror=

tar xvfz ISPConfig-3.0.1.6.tar.gz

cd ispconfig3_install/install/

El siguiente paso es ejecutar install.php para iniciar el instalador de ISPConfig 3.

```
[root@server1 install]# php -q install.php



--------------------------------------------------------------------------------

 _____ ____________ _____     __ _
|_  _/ ___| ___ \ / __ \   / _(_)
 | | \ `--.| |_/ / | / \/ ___ _ __ | |_ _ __ _
 | | `--. \ __/ | | / _ \| '_ \| _| |/ _` |
 _| |_/\__/ / |  | \__/\ (_) | | | | | | | (_| |
 \___/\____/\_|  \____/\___/|_| |_|_| |_|_|\__, |
```

```
          __/ |
             |___/
--------------------------------------------------------------------------------


>> Initial configuration

Operating System: Redhat or compatible, unknown version.

 Following will be a few questions for primary configuration so be careful.
 Default values are in [brackets] and can be accepted with <ENTER>.
 Tap in "quit" (without the quotes) to stop the installer.


Select language (en,de) [en]: <-- ENTER

Installation mode (standard,expert) [standard]: <-- ENTER

Full qualified hostname (FQDN) of the server, eg server1.domain.tld
[proyecto2.honey.com]: <-- ENTER

MySQL server hostname [localhost]: <-- ENTER

MySQL root username [root]: <-- ENTER

MySQL root password []: <-- yourrootsqlpassword

MySQL database to create [dbispconfig]: <-- ENTER

MySQL charset [utf8]: <-- ENTER
```

```
Generating a 2048 bit RSA private key
.....................................................................................+++
.....+++
writing new private key to 'smtpd.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]: <-- ENTER
State or Province Name (full name) [Berkshire]: <-- ENTER
Locality Name (eg, city) [Newbury]: <-- ENTER
Organization Name (eg, company) [My Company Ltd]: <-- ENTER
Organizational Unit Name (eg, section) []: <-- ENTER
Common Name (eg, your name or your server's hostname) []: <-- ENTER
Email Address []: <-- ENTER
Configuring Jailkit
Configuring SASL
Configuring PAM
Configuring Courier
Configuring Spamassassin
Configuring Amavisd
Configuring Getmail
Configuring Pureftpd
Configuring MyDNS
Configuring Apache
Configuring vlogger
Configuring Firewall
```

```
Installing ISPConfig
ISPConfig Port [8080]: <-- ENTER

Configuring DBServer
Installing Crontab
no crontab for root
no crontab for getmail
Restarting services ...
Stopping MySQL:          [ OK ]
Starting MySQL:          [ OK ]
Shutting down postfix:          [ OK ]
Starting postfix:          [ OK ]
Stopping saslauthd:          [ OK ]
Starting saslauthd:          [ OK ]
Shutting down Mail Virus Scanner (amavisd):    [ OK ]
Starting Mail Virus Scanner (amavisd):      [ OK ]
Stopping Courier authentication services: authdaemond
Starting Courier authentication services: authdaemond
Stopping Courier-IMAP server: imap imap-ssl pop3 pop3-ssl
Starting Courier-IMAP server: imap imap-ssl pop3 pop3-ssl
Stopping Courier-IMAP server: imap imap-ssl pop3 pop3-ssl
Starting Courier-IMAP server: imap imap-ssl pop3 pop3-ssl
Stopping Courier-IMAP server: imap imap-ssl pop3 pop3-ssl
Starting Courier-IMAP server: imap imap-ssl pop3 pop3-ssl
Stopping Courier-IMAP server: imap imap-ssl pop3 pop3-ssl
Starting Courier-IMAP server: imap imap-ssl pop3 pop3-ssl
Stopping httpd:          [ OK ]
[Wed Oct 28 16:24:17 2009] [warn] NameVirtualHost *:80 has no VirtualHosts
Starting httpd:          [ OK ]
Stopping pure-ftpd:          [ OK ]
Starting pure-ftpd:          [ OK ]
```

```
Installation completed.
[root@server1 install]#
```

El programa de instalación configura automáticamente todos los servicios subyacentes, por lo que no es necesaria la configuración manual

Ahora es posible acceder a ISPConfig 3 direccionando el navegador a http://proyecto2.honey.com:8080/ o http://192.168.1.38:8080/ e iniciar sesión con el nombre de usuario *admin* y la contraseña *admin*.

GLOSARIO

Análisis forense: “Es la técnica de capturar, procesar e investigar información con el fin de que pueda ser utilizada en la justicia”. (McKennish, 1998)

Evidencia digital: "Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático“. HB:171 2003 Guidelines for the Management of IT Evidence.

Honeypot: Un honeypot es un recurso que pretende ser un objetivo real. Se espera que un honeypot sea atacado o comprometido. Los objetivos principales son la distracción de un atacante y obtener información sobre un ataque y el atacante. "- R. Baumann, C. Plattner

"Un honeypot es un recurso del sistema de información cuyo valor reside en la intervención de usuarios no autorizados o el uso ilícito de ese recurso”. Lance Spitzner Fundador de The Honeynet Project.

Informática forense: Disciplina “que se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital, para luego ésta ser presentada en una Corte de Justicia”. ACURIO DEL PINO, Santiago. “Introducción a la informática forense”. Revista de derecho informático, alfa-redi, n° 110, septiembre, 2007