UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía, las Industrias y los Recursos Naturales no Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

Diseño e Implementación de una Honeynet para la red de datos de la Universidad Nacional de Loja, utilizando software Libre

"Tesis previa la obtención del título de Ingeniero En Sistemas"

Autor:

Heredia-Terán, Carlos-Mauricio

Director:

Ing. Ocampo-Carpio, Marco-Augusto, Mg. Sc.

Loja-Ecuador

2015

CERTIFICACIÓN DEL DIRECTOR

Ing. Marco Ocampo, Mg. Sc,
DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS

CERTIFICA:

Que el señor Carlos Mauricio Heredia Terán, egresado de la carrera de Ingeniería en Sistemas y cuyo tema versa "DISEÑO E IMPLEMENTACIÓN DE UNA HONEYNET PARA LA RED DE DATOS DE LA UNIVERSIDAD NACIONAL DE LOJA, UTILIZANDO SOFTWARE LIBRE", ha sido monitoreado, revisado y orientado bajo mi asesoramiento, por lo cual autorizo su presentación y sustentación.

Loja, 13 de Julio del 2015.

Ing. Marco Augusto Ocampo Carpio, Mg. Sc,
DIRECTOR DEL PROYECTO DE TESIS

AUTORÍA

Yo **CARLOS MAURICIO HEREDIA TERÁN**, declaro ser autor del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el Repositorio Institucional - Biblioteca Virtual.

Firma: 

Cédula: 1600464299

Fecha: 6/08/2015

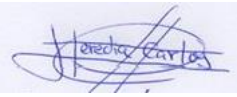
CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo **CARLOS MAURICIO HEREDIA TERÁN**, declaro ser el autor de la tesis titulada: **"DISEÑO E IMPLEMENTACIÓN DE UNA HONEYNET PARA LA RED DE DATOS DE LA UNIVERSIDAD NACIONAL DE LOJA, UTILIZANDO SOFTWARE LIBRE",** como requisito para optar el grado de: **INGENIERO EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja a los seis días del mes de agosto del dos mil quince.

Firma: 

Autor: Carlos Mauricio Heredia Terán

Dirección: Loja (Yaguarcuna. Cascarillas 26-60 y Buganvillas)

Teléfono: (07) 2103695 **Celular**: 0984697679

Correo Electrónico: cmherediat@unl.edu.ec - carlosherediat90@gmail.com

Director de Tesis: Ing. Marco Augusto Ocampo Carpio, Mg. Sc,

Tribunal de Grado: Ing. Jorge Iván Tocto, Mg. Sc.

Ing. Waldemar Victorino Espinoza Tituana, Mg. Sc.

Dr. Luis Fernando Paz Villaroel

DEDICATORIA

A mis padres, Elena Terán - Mauricio Heredia

A mi hermano, Bryan Heredia

AGRADECIMIENTO

La presente tesis es un esfuerzo, en el cual directa o indirectamente, participaron varias personas.

A mi familia, por su comprensión y apoyo, que me brindaron durante el desarrollo del proyecto. A la Ing. Lorena Conde, que con su experiencia y asesoría logré concretar con éxito el proyecto de tesis y con ello el proceso de titulación.

A la planta profesional que labora en la Unidad de Telecomunicaciones e Investigación de la Universidad Nacional de Loja, que estuvieron siempre prestos a brindar su ayuda en el desarrollo del proyecto de tesis.

A la planta docente, que con todos los conocimientos impartidos en las aulas de clase, me han permitido concluir de la mejor manera el presente proyecto fin de carrera.

CESIÓN DE DERECHOS

Carlos Mauricio Heredia Terán, autor del presente proyecto de titulación, autoriza a la Universidad Nacional de Loja, al Área de la Energía, las Industrias y los Recursos Naturales No Renovables y por consecuente a la carrera de Ingeniería en Sistemas, hacer uso total o parcial del contenido del mismo, en medida de lo que se vea conveniente.

a. Título

Diseño e Implementación de una Honeynet para la red de datos de la Universidad Nacional de Loja, utilizando software Libre

b. Resumen

Para el desarrollo del proyecto de tesis se realizó cuatro fases: describir la situación actual de la red de datos, mediante esta fase se logra determinar los puntos críticos que tiene la red de la UNL. La segunda fase consiste en analizar y seleccionar el tipo de Honeynet, la tercera fase es diseñar el diagrama de topología, donde será implementada la Honeynet tomando en cuenta los recursos Hardware que dispone la Universidad. Y finalmente la cuarta fase es la implementación y configuración de la Honeynet, para poder verificar el funcionamiento de la misma.

Se investigó casos de éxito en instituciones de educación superior, para identificar las ventajas de protección que brinda una Honeynet en la red de datos. Se determinó en base un estudio que el sistema operativo Linux Centos 7 (servidor) es una de las mejores alternativas para el correcto funcionamiento de una Honeynet.

Después de analizar y seleccionar el tipo de Honeynet (Virtual de 3ra Generación), en base a la situación actual de la red de datos de la UNL, se elaboró la topología de la Honeynet para su implementación y configuración. Al ser una Honeynet virtual solo necesita de un host anfitrión con el sistema operativo Centos 7, en el cual se van a levantar los elementos de la Honeynet: Honeypot (Centos 7), Honeywall (Honeywall CDROM) y Host Administrador (Centos 7), cada uno con su sistema operativo respectivamente.

Finalmente se realiza la fase de pruebas en un entorno real, capturando ataques mediante el funcionamiento correcto de la Honeynet.

Summary

In order to develop this thesis project four stages were carried out: the first involved a description of the current situation of the data network, this stage was achieved by determining the critical points that the UNL network has. The second stage is to analyze and select the type of Honeynet, the third one is to design the topology diagram, where the Honeynet was implemented taking into account the hardware resources available to the University. And finally the fourth stage is the implementation and configuration of the Honeynet to verify the operation of the aforementioned system.

Some studies done in institutions of higher education were investigated to identify the advantages of protection Honeynet provides in the data network. A study demonstrated that the Linux Centos 7 (server) operating system is one of the best alternatives to get the maximum potential of Honeynet.

After analyzing and selecting the type of Honeynet (Virtual 3rd Generation), based on the current state of the data network of the UNL, Honeynet topology for deployment and configuration was developed. Since Honeynet is virtual it only needs host with Centos 7 operating system, which will raise the elements of the Honeynet: Honeypot (Centos 7), Honeywall (Honeywall CDROM) and Host Manager (Centos 7) each with its own operating system respectively.

Finally the testing phase was done in a real environment, capturing data through the proper functioning of Honeynet.

Índice de Contenidos

Índice de Figuras

Índice de Tablas

c. Introducción

Las instituciones tanto públicas como privadas tienen entre sus bienes primordiales a la información que pueden generar. Actualmente debido a la sistematización que experimenta el mundo, la información cada vez es más pretendida, y por ende se encuentra propensa a ataques causados por agentes internos o externos, los cuales aprovechan las vulnerabilidades que poseen las redes de datos, para apoderarse de ella.

Debido a las vulnerabilidades y brechas de seguridad, se busca implementar una solución que permita contrarrestar los problemas de seguridad informática. Por ello, para la prevención o mitigación de cualquier tipo de amenaza es necesario conocer y comprender las vulnerabilidades del entorno. Una de las metodologías para esto es crear un ambiente de red controlado pero a la vez lo suficientemente atractivo para los atacantes, que permita detectar comportamientos maliciosos, para estudiarlos, entenderlos y actuar en consecuencia, ya sea de una manera proactiva o reactiva, sin perjudicar el ambiente de producción de la institución, siendo este el principio fundamental de una Honeynet.

La tecnología que nos permite conocer con detalle los ataques y vulnerabilidades de las redes son los Honeypots. Un Honeypot o “tarro de miel”, en el campo de la seguridad en redes de información, se define como un recurso de la red que se encuentra voluntariamente vulnerable para que el atacante pueda examinarla y atacarla. Directamente no es la solución a ningún problema; su función principal es recoger información importante sobre el atacante que permita prevenir estas incursiones dentro el ámbito de la red real en casos futuros.

El presente proyecto fin de carrera consiste en implementar un tipo especial de Honeypot denominado “Honeynet” con el objetivo de reunir información sobre la actividad del intruso. Logrando así detectar las vulnerabilidades que posee nuestra red antes de que estas sean explotadas, además de conocer los riesgos a los cuales nuestros sistemas de producción están expuestos. Una de las ventajas de las Honeynets es que nos proveen de la inteligencia necesaria para conocer los riesgos que tiene la red. El concepto en el que se centran las Honeynets es que permiten estar un paso adelante del enemigo, permitiendo así aprender cuanto sea posible de las amenazas y del comportamiento de los atacantes, para implantar una arquitectura de

seguridad proactiva que nos permita no sólo defendernos de tales amenazas, si no también someterlas antes de que sucedan..

Fases que permitieron cumplir con los objetivos planteados en el proyecto de tesis: Analizar la situación actual de la red de datos de la UNL para determinar sus puntos críticos, la revisión de casos de éxito de instituciones de educación superior que utilizan una Honeynet, permitió realizar el diseño de la solución una Honeynet Virtual de 3ra Generación, continuando con la implementación en la red de datos de la UNL, y validando mediante pruebas de rendimiento el correcto funcionamiento de la Honeynet.

En este informe se presenta, en primera instancia una Revisión de Literatura, que consiste en la recolección teórica de los puntos clave del proyecto de tesis, se destacan la arquitectura y los tipos de Honeynet. El apartado de Materiales y Métodos, describe en su totalidad los recursos materiales, científicos y metodológicos que se necesitaron para el desarrollo del proyecto. El apartado de Resultados presenta el desarrollo de las Fases establecidas por el proyecto, iniciando con el proceso de Análisis, hasta la implementación y pruebas de la solución. En el apartado de Discusión se presenta un contraste de como los resultados obtenidos, cumplen con los objetivos planteados como metas en el proyecto de tesis. El apartado de Conclusiones presenta una descripción de cómo se evidencian los resultados, en base a la experiencia obtenida en el desarrollo del proyecto. Y la sección de Recomendaciones presenta una lista de sugerencias, que se pueden tomar en cuenta para ampliación o estabilidad de una Honeynet.

d. Revisión de Literatura

1 Introducción a la Honeynet

La tecnología que nos permite conocer con detalle los ataques y vulnerabilidades delas redes son los Honeypots. Un Honeypot o “tarro de miel”, en el campo de la seguridad en redes de información, se define como un recurso de la red que se encuentra voluntariamente vulnerable para que el atacante pueda examinarla, atacarla [1].

Directamente no es la solución a ningún problema; su función principal es recoger información importante sobre el atacante que permita prevenir estas incursiones dentro del ámbito de la red real en casos futuros.

El presente proyecto consiste en implementar un tipo especial de Honeypot denominado “Honeynet” con el objetivo de reunir información sobre la actividad del intruso. Logrando así detectar las vulnerabilidades que posee la red antes de que estas sean explotadas. Una de las ventajas de las Honeynets es que nos proveen de la inteligencia necesaria para conocer los riesgos con los que se cuenta en la red.

El concepto en el que se centran las Honeynets es que permiten estar un paso adelante del enemigo, permitiendo así aprender cuanto sea posible de las amenazas y del comportamiento de los atacantes, para implantar una arquitectura de seguridad proactiva que nos permita no sólo defendernos de tales amenazas, si no también someterlas antes de que sucedan [2].

1.1 Honeynet

Antes de analizar el concepto de una Honeynet es preciso definir que es un Honeypot “Un Honeypot es un recurso computacional altamente monitoreado, el cual se desea que sea probado, atacado o comprometido” [3]. De una manera más clara también se lo define como: recurso de un sistema de información, cuyo valor reside en el uso no autorizado o lícito del mismo” [2], es decir un Honeypot es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas.

Una vez aclarado este concepto se puede definir a una Honeynet como un Honeypot de alta interacción que consta de una red de sistemas, cuyo propósito es ser comprometida por algún usuario malicioso, con la finalidad de aprender sobre las herramientas, tácticas y motivos que alientan a este tipo de usuarios. Esta red captura y controla mediante un

firewall todo el tráfico destinado a los equipos dentro de ella para su posterior análisis. La finalidad es crear una infraestructura en la que no solo haya sistemas reales, sino servicios reales tales como DNS, HTTP, SMTP, etc. que permitan al intruso estar en un ambiente más realista, pero controlado.

Las Honeynets son herramientas de seguridad con un punto de vista diferente al tradicional, que es un comportamiento defensivo, tradicionalmente se intenta defender de ataques una red, mediante cortafuegos, medios de cifrado o sistemas de detección de intrusos (IDS). Los Honeynets son herramientas diseñadas básicamente para aprender y adquirir experiencia en el área de seguridad [4].

1.1.1 Tipos de Honeypots

Una clasificación de Honeypots puede basarse en el nivel de interacción que tendrá el atacante con el Honeypot. Recordemos que mientras el atacante genere más actividad en el Honeypot mas aprenderemos de ello, sin embargo cuando un Honeypot tenga un alto grado de interacción, existirá un mayor riesgo de comprometer a otros sistemas a partir de él [2].

Los Honeypots se clasifican de acuerdo a las formas en que agregan valor de seguridad y reducen el riesgo en la organización [2, 5].

1.1.1.1 Honeypot de Producción

Proporcionando así servicios similares a la verdadera red. Su objetivo es debilitar el riesgo de un ataque a la red productiva de la organización, de tal manera que ayude asegurar sistemas y redes con la prevención, el engaño y la disuasión de los atacantes, desviándolos de su objetivo real hacia el señuelo. Con lo cual se puede prevenir cualquier ataque hacia la red real (denegando cualquier acceso con un origen determinado, limitando las capacidades de un servicio o paralizando servicios momentáneamente en el caso de ser posible), logrando tener un detalle de los métodos, herramientas usadas por los atacantes en los sistemas, es decir un Honeypot de Producción cumple el rol de capturar y defender [2, 5].

1.1.1.2 Honeypot de Investigación

Proteger los sistemas contra nuevas amenazas. Es principalmente usado para investigación en instituciones como Universidades, organizaciones gubernamentales, militares. En otras palabras, el Honeypot de Investigación cumple la función de capturar información para ser analizada [5].

Además se usan para recolectar información sobre los movimientos de los intrusos, es decir, se registra cada movimiento del atacante para usar esta información y crear perfiles de los mismos [6].

Existe otra clasificación que divide ambos tipos de Honeypots, que se basa en el grado en el que se compromete o arriesga a la red real:

- *Honeypots de baja interacción:* Emulan servicios, su instalación es del tipo "plug and play"[3], al emular servicios constituyen un sistema controlado por consiguiente el riesgo inmerso es limitado. Los servicios no son reales y no representan un riesgo como tal por su capacidad limitada. Su principal desventaja es la limitación de la cantidad de información recogida, ya que no permite un mayor nivel de interacción con el atacante, este queda limitado en su ataque y solo muestra quizá lo que sería uno de sus primeros para el ataque [2, 5, 6]. Entre los más comunes Honeypots de baja interacción tenemos: Nepenthes, Honeyd, Honeytrap, Tiny Honeypot.
- *Honeypots de alta interacción:* Son difíciles de implementar y mantener, porque los sistemas y servicios que brinda no son emulados, son reales montados sobres sistemas operativos y hardware, lo que aumenta el riesgo en su uso. La ventaja que se obtiene al montar esta solución es la gran cantidad de información que se puede recoger del atacante, según la complejidad del Honeypot, podemos ser capaces de conocer exactamente todos los pasos del intruso, sus técnicas y sus herramientas. Como el riesgo aumenta, se hace necesario implementar controles que eviten que el Honeypot se convierta en una plataforma de ataque [2, 5, 6].

Otra clasificación para los Honeypots se basa en su implementación, se distinguen dos tipos: Honeypots Físicos y Honeypots Virtuales [7].

- **Los Honeypots Físicos**: son implementados en una maquina física real, lo que lo convierte en un Honeypot de alta interacción el cual puede ser comprometido totalmente. Como constituyen una maquina real, normalmente son más caros y complejos en su implementación [7].
- **Honeypots Virtuales:** Los Honeypots Virtuales nacen de la necesidad de tener un gran espacio de direcciones IP, es casi imposible implementar un Honeypot por cada IP por razones en espacio físico y económico. En una maquina física (Host), se puede levantar varios Honeypots como máquinas virtuales, los

Honeypots no constituyen una maquina real, pero pueden proporcionar todo el nivel de interacción como un Honeypot Físico de Alta Interacción, la única diferencia es que está corriendo bajo algún software de virtualización y comparten los recursos físicos de la máquina real, inclusive la conexión a internet, permitiendo tener conectadas a toda una red de Honeypots con sus respectivas IPs dentro de una máquina física, facilitándonos la movilidad y reduciendo enormemente la cantidad de hardware usado [7, 8].

1.1.2 Uso de la Honeynet

Cuando se usan en conjunto con otros mecanismos de seguridad. Al recoger información de las intrusiones y estudiarlas podemos conocer nuevas amenazas y herramientas aún no documentadas, determinando así patrones de ataque y los diferentes motivos de los intrusos [8].

Las Honeynets son una herramienta, y puede ser usada para otros fines, como comprobar y desarrollar la capacidad de respuesta ante cualquier incidente. En las universidades pueden ser usadas para estudiar tipos y patrones de ataque o simplemente para investigar amenazas como función principal [8].

2 Arquitectura de la Honeynet

Una arquitectura es el diseño conceptual y la estructura operacional fundamental de un sistema. Es decir, es un modelo y una descripción funcional de los requerimientos y las implementaciones de diseño para los diferentes elementos que conforman una Honeynet.

Las Honeynets no son un producto, son toda una arquitectura, una red con un ambiente totalmente controlado, dentro de ella tenemos a los sistemas que son los objetivos. La Honeynet es como una pecera con servidores, routers, computadores personales, y todos los elementos de una red común dentro de ella como elementos, mientras nosotros vemos como los atacantes interactúan con ellos [8, 9].

Para mantener el ambiente controlado la clave en la arquitectura de la Honeynet es su Puerta de Salida (Gateway) llamado Honeywall. Este dispositivo separa la Honeynet del resto del mundo. Por el Honeywall atraviesa todo el tráfico desde y hacia la Honeynet.

El Honeywall es un dispositivo que originalmente era de Capa 3 pero actualmente puede ser un bridge invisible de Capa 2. Tiene tres interfaces de red (eth0, eth1, eth2) como se muestra en la Figura 1; las dos primeras (eth0, eth1), como puertas de entrada y salida, forman el bridge de Capa 2 separando la Honeynet con el mundo, y una tercera interface de red opcional que sirve para administración [8, 9].

Figura 1: Arquitectura de la Honeynet [8].

Para crear una arquitectura correctamente el Honeynet Project ha definido unos requisitos que garantizaran el correcto funcionamiento de la Honeynet y mantener un ambiente seguro para los sistemas contiguos a la red. Estos requisitos son: control de datos, captura de datos y recolección de datos [9].

2.1 Control de Datos

El control de datos en una Honeynet se encarga de mitigar o de bloquear todo riesgo que se produzca desde los Honeypots hacia el mundo. Es importante que la Honeynet no sea usada por los atacantes como un arma o herramienta de ataque hacia otros sistemas productivos.

Recordar que en la Honeynet se usan sistemas no emulados, lo cual eleva el riego de ser usado como herramienta de ataque. Se debe definir qué nivel de riesgo se va manejar en la Honeynet, entre mayor sea el riesgo, mayor será la cantidad de datos obtenidos del atacante porque está aumentando la libertad con la que él puede interactuar con los sistemas.

El Control de Datos es el requerimiento más importante en una Honeynet y es imprescindible que por ningún motivo se deje abierto el acceso directo sin restricciones desde y hacia los Honeypots en una Honeynet. En otras palabras el control de datos debe actuar de manera 'fail-close' [5], lo que significa que si este falla por cualquier motivo inclusive el de ser blanco de un ataque, al caer el sistema de control de datos la Honeynet quede totalmente bloqueada de la red. La implementación del control de datos debe ser la suma de diferentes mecanismos sobrepuestos como capas para evitar un punto único de fallo. Dependiendo de los tipos de Honeynet pueden ser: Gateway IDS, restricciones en consumo de ancho de banda, contador de conexiones. A medida que las generaciones de Honeynet vayan madurando se desarrollarán nuevas técnicas de bloqueo.

2.2 Captura de Datos

La captura de datos consiste en el monitoreo y registro de toda la actividad de los atacantes con los Honeypots. Al igual que el control de datos, la captura debe ser implementada en capas, proporcionando varios niveles y tipos de captura. Distintos mecanismos de captura deben agruparse, proporcionando una mayor gama de tipo de datos capturados y previniendo también los puntos ´únicos de fallo. Estos mecanismos pueden ir desde un simple sniffer que registre todos los datos que pasan por la red,

hasta un complejo sistema que permita registrar datos sobre canales encriptados como IPSec, SSH, SSL [8-10].

Dentro de la captura de datos se debe analizar el lugar para almacenar la información recolectada, la cual no debe grabarse en forma local sino debe ser registrada y almacenada en un sistema seguro separado de los Honeypots [8-10].

2.3 Recolección y Análisis de Datos

La recolección de datos está planteada para el caso en que se tengan varias Honeynets en un entorno distribuido. Puede ser a nivel nacional o en varios sectores centralizando los datos recogidos [8-10].

El análisis es el punto en el que los datos recogidos por la Honeynet son analizados y estudiados en busca de patrones de ataque, ataques nuevos y lo que se haya definido como objeto de investigación.

Es decir la recolección de datos es la parte de recopilación de toda la información captada por la interacción de la Honeynet dentro de la red. El usuario debe clasificar la información útil para cumplir los objetivos planteados o la teoría que se pretende demostrar.

3 Tipos de Honeynets

Siguiendo los requisitos de una Honeynet se han implementado y desarrollado tres generaciones, las cuales se diferencian en los métodos y técnicas que se usen para implementar dichos requisitos.

3.1 Honeynets de Generación I

Fue la primera arquitectura desarrollada por el Honeynet Project en 1999 y se mantuvo hasta finales del año 2001. Se compone de una máquina Gateway[1] (llamada firewall[2]) responsable del control de datos y otra denominada (IDS: Intrusion Detection System /Sistema de detección de intrusos) que es responsable de la captura de datos [8].

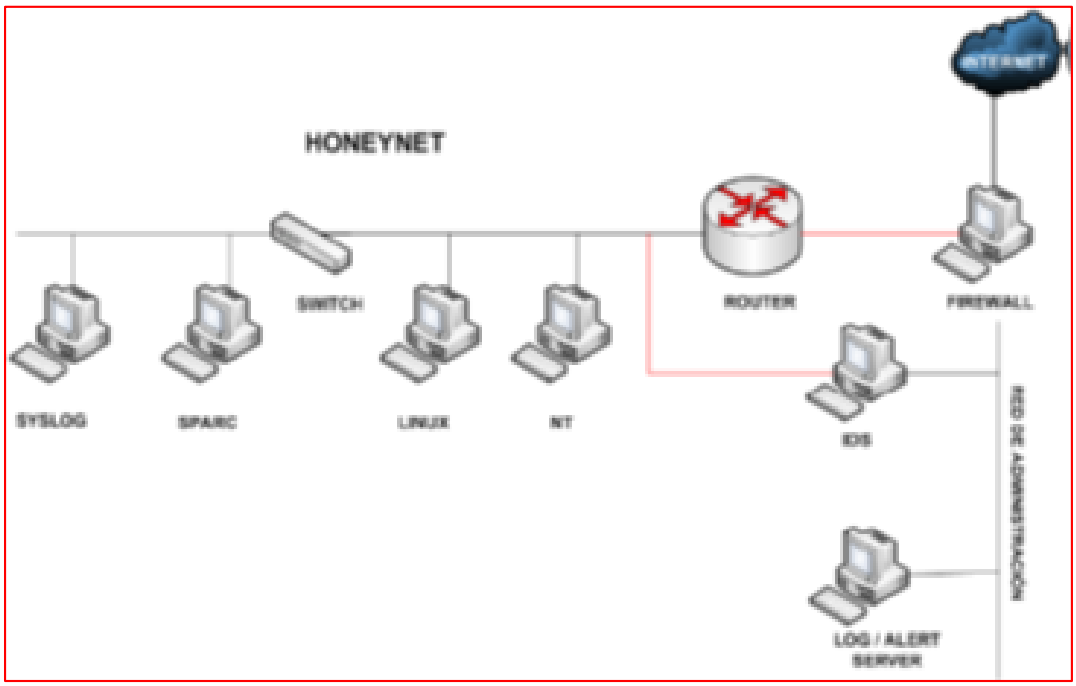


Figura 2: Honeynet de Generación I [8]

Como se muestra en la Figura 2, la máquina firewall dispone de 3 interfaces de red (interna, externa y administración), la interfaz externa es usada para conectarse a Internet, la interfaz interna para conectarse a la Honeynet y la última para conectarse con el servidor de logs[3], todas las conexiones desde y para la Honeynet pasan a través de esta máquina Gateway [5, 8, 9].

[1] Gateway: Una pasarela o puerta de enlace, es un dispositivo que permite interconectar redes.
[2] Firewall: Es un sistema de defensa que se basa en la instalación de una “barrera” entre el PC y la red.
[3] Logs: Registro de actividad en un sistema.

La interfaz de administración simplemente se usa para configuraciones y recolección de logs en el firewall. El dispositivo IDS/Sniffer[4] posee dos interfaces, una posee una dirección IP y es utilizada para el manejo y recolección de datos. Y la otra no posee dirección IP por donde se realiza el sniffing, por lo que al ser configurada de esta forma es más difícil de detectar y atacar directamente [8, 9].

En esta arquitectura el principal elemento de defensa de la red es el Firewall, por lo que se requiere de una mayor configuración. Las principales características del Firewall en este tipo de arquitectura son [8]:

- Opera en capa 3 (tiene asignado direcciones IP) lo cual lo hace visible para el Internet y desde la red interna.
- Usa NAT (Network Address Translation).
- TTL (Tiempo de Vida en Saltos) de los paquetes sufren un decremento, lo cual lo hace más fácil de detectar, pero al ser una pasarela para la red se puede configurar para que actúe como un firewall normal con las reglas de reject, drop, silently y forward sobre las conexiones. Además se pueden controlar el número de conexiones permitidas, lo cual ayuda en el control de datos.

3.1.1 Control de Datos (Generación I)

El principal objetivo del control de datos es disminuir el riesgo de ataques desde un Honeypot comprometido hacia una red productiva, es por esta razón que se deben aplicar reglas sobre las conexiones salientes. En este tipo de arquitectura los dispositivos que intervienen son el Firewall/Gateway y el router. El control de datos está dividido dentro de dos categorías [8-10].

- **Connection Blocking:** Previene las conexiones excesivas desde la Honeynet, el grado de aceptación o denegación estará directamente relacionado con lo que uno quiera aprender y el riesgo que se desee asumir, debido a que permitir mayores conexiones nos brinda la posibilidad de aprender más pero también genera más riesgos, debido a que se encuentra configurado conjuntamente con la red de producción.
- **Connection Limiting:** Tiene como objetivo mitigar inundaciones por conexiones salientes, limitando anchos de banda, etc. El router se instala detrás del firewall, proporcionando un filtrado extra a los paquetes y sirve de respaldo en caso de

[4] Sniffer: Técnica por la cual se puede “escuchar” todo lo que circula por una red.

fallos en el firewall, además también se instala con la finalidad de ocultar el firewall/Gateway de los ojos de un atacante desde un Honeypot comprometido, de manera que si se investiga el Gateway del Honeypot, el atacante verá al router y no al firewall.

3.1.2 Captura de Datos

Los dispositivos que intervienen en la captura de datos son: el firewall, el IDS y los Honeypots. La captura de datos nos permite recolectar y almacenar la evidencia tanto de la actividad de la red como de las máquinas intervinientes en los ataques a los que fueron expuestos. La captura de datos, no es solamente almacenar el log o el tráfico de red, sino que es una combinación de monitoreo de la actividad, observación como opera el atacante y la capacidad de reconocer las técnicas que usa este [8, 10].

Las categorías de tecnologías para la captura de datos pueden estar agrupadas en 4:

- Almacenamiento de las transacciones de red: IP de origen y destino, protocolos y puertos involucrados.
- Almacenamiento del tráfico de red: Usualmente todo el tráfico en binario.
- Almacenamiento de la captura del HOST: Todo lo relativo a la actividad realizada en el host por el/los atacantes (puede incluir: imágenes del disco duro, logs del S.O., etc.).
- Alertas de los IDS: Este es el más importante de todos y aunque esté basado en el tráfico obtenido, es donde las reglas definidas para los distintos patrones de tráfico nos permiten encontrar y/o tomar medidas.

3.2 Honeynet de Generación II

Este segundo modelo dentro de las generaciones de las Honeynets fue lanzado y ha sido usado desde principios del 2002 por el Honeynet Project. En relación a su antecesora, esta arquitectura introduce una serie de modificaciones, las cuales se enfocan en aumentar la interacción con el atacante para aumentar la cantidad y calidad de datos recolectados. Para esta tarea fue necesario ocultar mejor los sistemas haciéndolos prácticamente indetectables.

Como se muestra en la Figura 3, esta arquitectura es mucho más sencilla que la presentada en la Generación I, las tareas de control y captura de datos ahora están centralizadas en un solo dispositivo llamado Honeywall lo que permite que esta arquitectura sea fácil de desarrollar y mantener [8, 10].

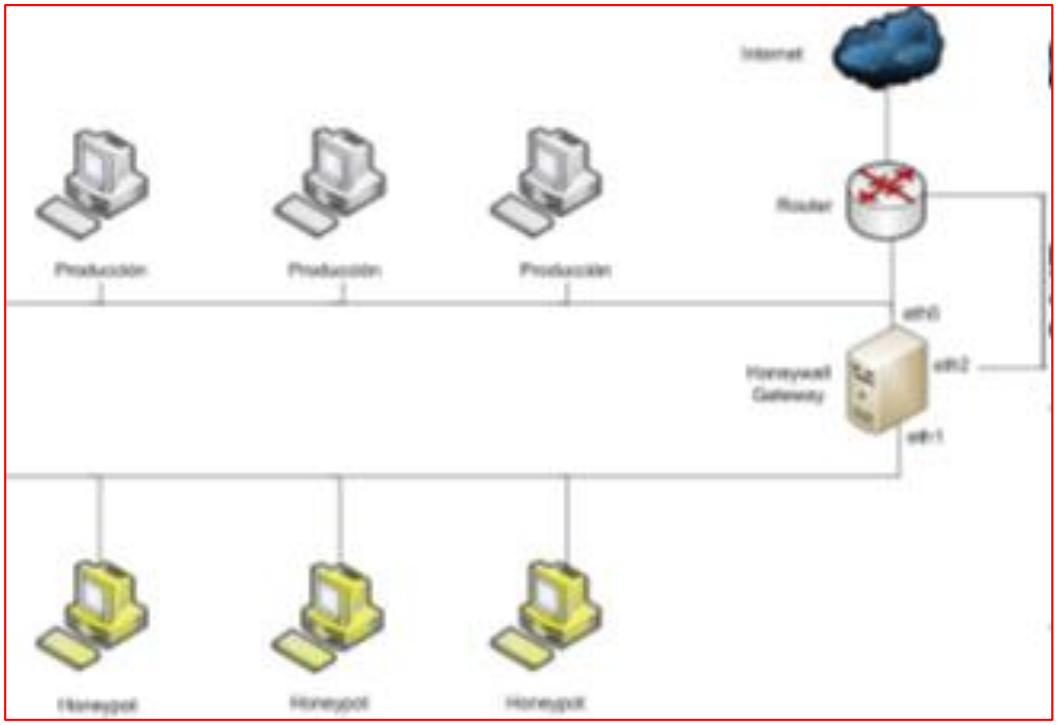


Figura 3: Honeynet de Generación II [8]

El Honeynet Gateway (Honeywall) es un dispositivo con tres interfaces de red: eth0, eth1, eth2. La interface externa (eth0) del Honeywall se conecta con el sistema de producción, la interface interna (eth1) se conecta con la Honeynet, ambas están a modo de puente (bridge) transparente lo cual significa que no poseen una pila de IP, ni MAC asociadas, no realizan encaminamiento, ni decrementan el TTL de los paquetes que las atraviesan.

La tercera interfaz (eth2) sí tiene una dirección de IP y es conectada a una red segura con fines de administración y recolección de datos. El comportamiento del Honeywall como dispositivo de Capa 2 (Bridge) transparente, dificulta enormemente su detección por parte de los atacantes y permite la integración de la Honeynet a la red de Producción e incluso compartir Vlan con otros sistemas dentro de la organización en la que se esté implantando. Esta integración permite el estudio de ataques internos y externos en los sistemas de producción, en el caso de la Generación I esta tarea se dificulta porque se tienen dos redes (Honeynet, Producción) totalmente aisladas [8, 10].

3.2.1 Control de Datos

Para mejorar la arquitectura de la Generación I, la cual usaba un firewall que trabajaba en capa 3, que lo hacía fácilmente detectable, se resolvió hacer un gateway de capa 2

transparente, el cual es mucho más difícil detectar. En este único dispositivo va funcionar el control de datos de nuestra Honeynet, será un firewall que controle y cuente todas las conexiones que entran y salen pero ahora en modo BRIDGE [8].

Se agrega una nueva capa al Control de Datos, un sistema de prevención de Intrusos NIPS. El NIPS trabaja de la misma forma que un IDS, tiene la capacidad de analizar en tiempo real un paquete, usa una base de datos de firmas con ataques conocidos, si el paquete coincide con un ataque este puede ser bloqueado o modificado para hacerlo inofensivo, para mejorar la interacción con el atacante y hacer más invisible el sistema se puede modificar los paquetes, permitiendo al intruso ejecutar sus ataques pero sin llegar a afectar a los sistemas comprometidos.

Los NIPS bloquean o modifican ataques que sean conocidos y configurados en su base de datos, pero para ataques nuevos no representan una barrera. En este caso entra la primera capa del control de datos que viene de la Generación I y el Honeywall bloqueará paquetes utilizando el conteo de conexiones inhabilitando cualquier ataque que supere el umbral configurado [8].

3.2.2 Captura de Datos

Para la captura de datos las Honeynets Gen II empelan las mismas tácticas que en Gen I con mejoras en los métodos y herramientas, la recolección de la información es efectuada en tres capas: el firewall, el IDS y los Honeypots [8-10].

La captura de datos es llevada a cabo por el IDS residente y el firewall. Los logs del firewall nos brindan información acerca de todas las conexiones entrantes y salientes, y por otro lado, el IDS nos da alertas sobre los patrones de ataques conocidos, esta primera etapa nos informa acerca de toda la actividad dentro de la Honeynet [8-10].

Con el objeto de obtener un panorama más amplio de toda la actividad, involucramos a toda la información suministrada por el Honeypot a través de sus logs, logrando de esta manera tener nuestra tercera capa de captura de información [8-10].

3.3 Honeynets de Generación III

Esta arquitectura se dio a conocer a inicios del 2005. Con respecto a su antecesora es muy similar, ya que mantiene los mismos dispositivos y características. Mejora las versiones de las herramientas usadas y su principal objetivo es analizar los datos recogidos [8-10].

En la Honeynet de Segunda Generación se tuvo dificultad al analizar los datos recogidos, puesto que cada herramienta en cada capa de recolección de datos manejaba su propio formato, y no se los podía vincular entre ellos de una manera simple. Por ejemplo si existe un ataque se debe rastrear su tiempo de vida en todos los niveles de captura, se analizan los datos por separado, lo que consume mucho tiempo, debido a que se tienen archivos pcap, logs de sistemas, y registros en base de datos que deben ser vinculados unos con otros.

La Segunda Generación en Captura de datos presentaba limitantes puesto que no se definía un formato de recolección, al no tener una relación en la estructura de esos y al no poseer un API[5] que facilite la tarea de análisis. Cada fuente de datos tiene unos datos en formato independiente, todo esto simplemente retrasaba la tarea de investigación, por estas razones nace un nuevo requisito, el análisis de datos [8].

El análisis de datos en la Generación III, unifica todos los datos registrados por cada herramienta de la captura de datos relacionándolos con los datos proporcionados por el control de datos, de esta forma podemos saber precisamente qué conexión generó una alerta y seremos capaces de rastrear todos los paquetes que están relacionados a esa conexión [11].

Si un atacante supera el límite de conexión usando SSH[6], esto generará una alerta. En el análisis se podrá identificar cuál fue el paquete exacto que fue bloqueado, cuantos paquetes están involucrados en esta conexión, cuál es la IP origen de los paquetes, qué tipo de S.O usa el atacante, y cuáles han sido los comandos ejecutados sobre el Honeypot comprometido [8, 10, 11].

Todos estos datos ahora los tenemos relacionados pero proceden de fuentes y herramientas distintas. Para poder unificar formatos, algunas de las herramientas usadas en la captura de datos han sido modificadas y actualizadas, como es el caso del Sebek[7], SEC[8], etc.

[5] API: Aplicaciones de Interfaces de Programación.
[6] SSH: Conexión remota encriptada.
[7] Sebek: Herramienta diseñada para capturar datos.
[8] SEC: Herramienta de correlación de eventos que permite gestionar una gran cantidad de información en base a patrones.

3.4 Honeynets Virtuales

Una Honeynet Virtual se basa en el mismo concepto de la Honeynet pero implementándose dentro de un mismo computador, todos sus dispositivos son virtualizados mediante un software que permita esta tecnología [4, 8-10].

Dentro de una máquina física se levantan los Honeypots como máquinas virtuales formando la Honeynet Virtual. Dependiendo de la configuración de cada uno, y de la arquitectura de red, podríamos hablar de Honeynets virtuales de I, II, III generación. La idea de virtualizar el sistema es reducir costos por requerimiento de dispositivos, entre más grande es la Honeynet, más dispositivos y espacio físico se necesita. En una Honeynet Virtual todo se encuentra en una sola máquina física. En el caso de aumentar más dispositivos virtuales simplemente se mejora el hardware de la máquina anfitriona.

Entre las limitaciones tenemos: el hardware necesario de la máquina que alberga a la Honeynet, el software que es usado para virtualizar, si el atacante toma en su poder la máquina anfitriona tendría control sobre toda la Honeynet y sería un peligro para los sistemas reales. Las Honeynet Virtuales se dividen en dos grandes tipos: AutoContenidas e Híbridas [4, 8-10].

3.4.1 Honeynet Virtual Autocontenida

La Honeynet virtual Autocontenida engloba a una Honeynet en un solo equipo. La red entera está virtualmente contenida en un único y físico sistema. Una red Honeynet típicamente consiste de un cortafuego para Control de Datos y Captura de Datos, y los Honeypots dentro de la Honeynet.

Un esquema de esta clase de Honeynet sería la que muestra la figura que aparece a continuación [4].

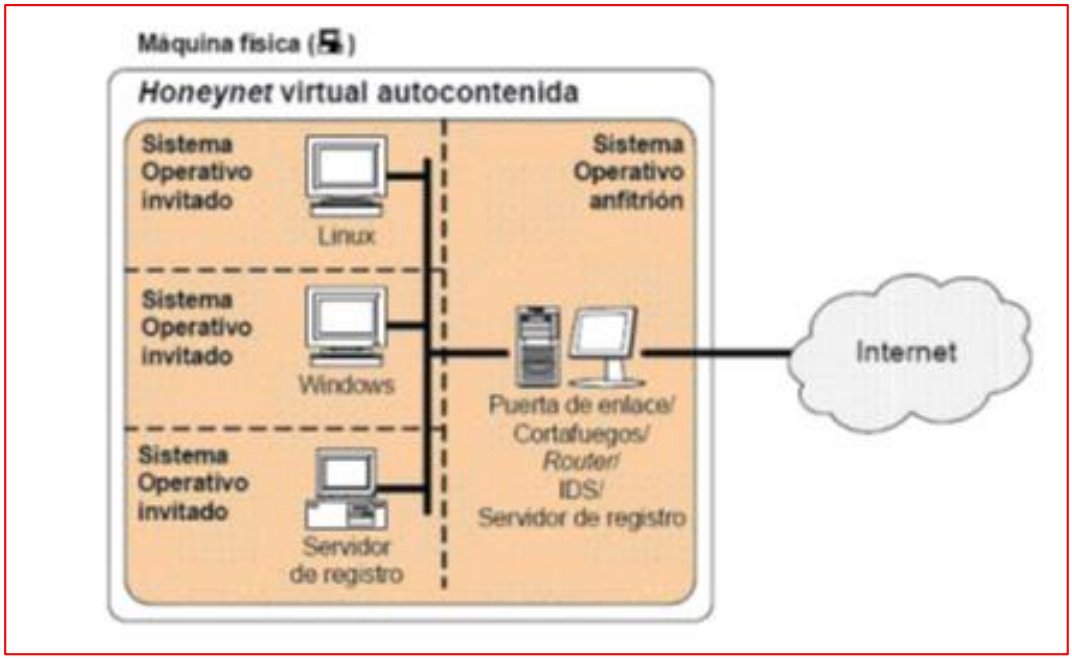


Figura 4: Esquema de Honeynet Virtual Autocontenida [8]

Las ventajas que presentan este tipo de Honeynet virtuales son:

- Fácilmente transportable, especialmente si se instala en un portátil.
- Rápida puesta en funcionamiento. Una vez instalada, sólo hay que conectarla a la red y configurarla en pocos minutos.
- Es barata y ocupa poco espacio. Sólo nos hace falta un ordenador.

Las desventajas que presentan este tipo de Honeynet virtuales son:

- Si falla el hardware, la Honeynet entera podría dejar de funcionar.
- Necesidad de un ordenador de altas prestaciones. Aunque sólo requiere un ordenador, tiene que tener suficiente memoria y capacidad de procesador.
- Seguridad. Como todos los sistemas comparten el mismo hardware, puede que un atacante acceda a otras partes del sistema. Tiene mucha dependencia del software virtual.
- Limitación por software. Como todo tiene que ejecutarse en una sola máquina, hay software que no se podrá utilizar por problemas de incompatibilidad. Por ejemplo un sistema operativo de cisco en una máquina con un procesador de Intel.

3.4.2 Honeynets Híbridas

Llamadas híbridas por combinar una Honeynet Clásica con una Honeynet Virtual, se agrega un dispositivo adicional en la arquitectura. Uno sirve como Honeywall (punto de entrada, control y recolección de información de la Honeynet) y otro levanta la red virtual de Honeypots [4, 8].

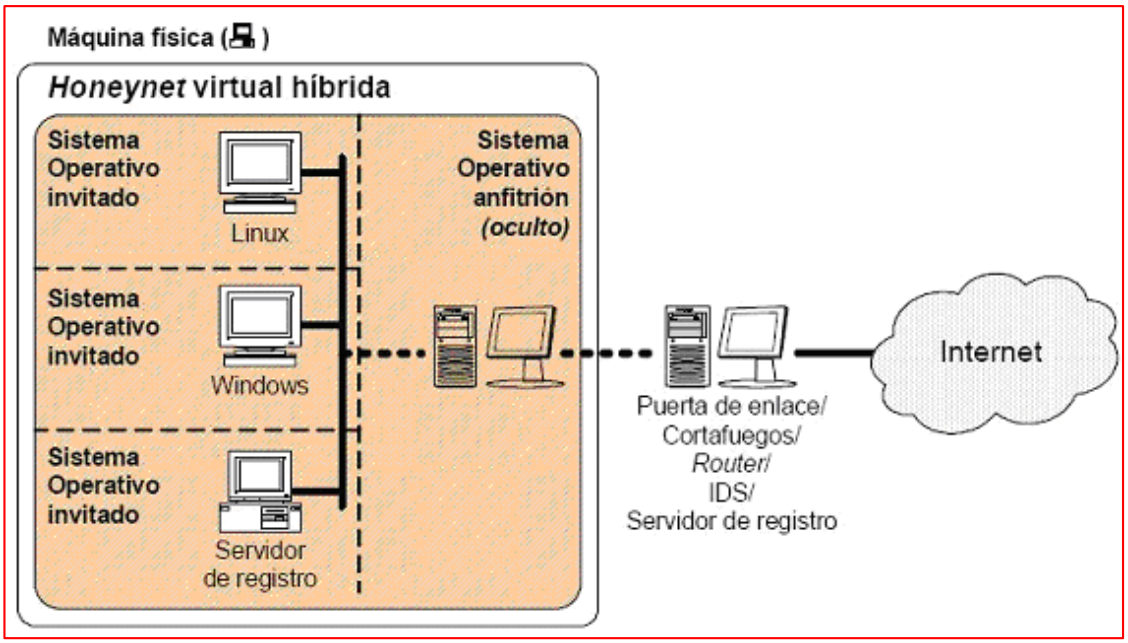


Figura 5: Esquema de Honeynet Virtual Hibrida [4].

Ventajas:

- Seguridad: eliminan el punto único de fallo y aíslan los datos y el control en otro dispositivo.
- Flexible: se tiene un dispositivo que contienen diferentes tipos de Honeypot que son máquinas virtuales, las cuales pueden ser de diferentes tipos con diferentes servicios, fáciles de copiar, borrar, duplicar, lo que facilita enormemente en la tarea de administración. Si se daña un Honeypot sólo hay que levantar un duplicado ya pre instalado.

Desventajas:

- Se dificulta la movilidad: debido a que tenemos dos dispositivos.
- Costosas: se incrementa el costo por hardware y en espacio.

Para cualquier tipo de Honeypot o Honeynet Virtual hay que considerar que pueden ser usadas técnicas de fingerprinting (obtención del tipo y versión del sistema operativo mediante el envío de paquetes IP específicamente construidos) sobre los Honeypots revelándole al atacante la virtualización de los sistemas [12].

4 Herramientas de la Honeynet

4.1 Sistema Detector de Intrusos (IDS)

Esta herramienta que detecta accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, que usan herramientas automáticas. El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas [8-10, 13].

Snort: Snort es un Sistema de detección de intrusiones de red, open source, capaz de realizar análisis de tráfico en tiempo real y loggin de paquetes sobre redes IP. Esta herramienta permite realizar análisis de protocolos, búsqueda/coincidencia de contenido y puede ser usado para detectar una gran variedad de ataques, siempre y cuando las reglas de Snort definan la detección de dichos ataques. Además, este IDS permite que reglas existentes puedan ser instaladas y que nuevas reglas puedan ser creadas, para detectar los diferentes ataques [14].

4.2 SEC (Simple Event Correlator)

SEC es una poderosa herramienta de correlación de eventos que permite gestionar una gran cantidad de información en base a patrones, lo que permite diseñar alarmas a medida y en función de las alertas que se vayan generando. La correlación de eventos es un procedimiento donde se procesa una secuencia de eventos, con el fin de detectar a ciertos grupos de eventos que ocurren dentro de un mismo intervalo de tiempo redefinido. SEC es un correlacionado de eventos ligero que se ejecuta como un proceso único y sigue la filosofía UNIX [8, 9, 13].

La importancia su empleo en este proyecto, consiste en la determinación de falsos positivos. Las diferentes herramientas de detección de intrusiones y análisis de conexiones proporcionan los logs determinados de cada intrusión. En este punto SEC se encarga de determinar que logs realmente pertenecen a un ataque (y no son parte de actividades normales que ocurren en la red), y de generar alertas [8, 9, 13].

4.2.1 Descripción de SEC

SEC es una herramienta ideal para el monitoreo de la red en tiempo real, su estructura y elementos se detallan a continuación.

Tipos de Reglas Los tipos de reglas que presenta SEC son los siguientes:

- Single
- SingleWithScript
- SingleWithSuppress
- Pair
- PairWithWindow
- SingleWithThreshold
- SingleWith2Thresholds
- Suppress
- Calendar

Los tipos de reglas que se van a emplear en este proyectos son los siguientes:

- **Single:** Utilizado para detectar eventos de entrada coincidentes, y ejecutar una acción inmediatamente.

- **SingleWithThreshold:** Empleado para contar el número de eventos de entrada coincidentes, ocurridos durante un tiempo t (segundos) determinado. Si el umbral de eventos dado es excedido, se ejecuta una acción y se ignora el resto de eventos coincidentes durante el resto de la ventana de tiempo. El proceso continua ejecutándose hasta cuando la ventana de tiempo expira sin ninguna coincidencia de eventos.

5 Virtualización

Virtualización es un término amplio que se refiere a la abstracción de los recursos de una computadora. Este término es bastante antiguo y su uso se remonta a años anteriores a 1960, y ha sido aplicado a diferentes aspectos y ámbitos de la computación, desde sistemas computacionales completos hasta capacidades o componentes individuales. El tema en común de todas las tecnologías de virtualización es la de ocultar los detalles técnicos a través de la encapsulación. La virtualización crea una interfaz externa que esconde una implementación subyacente mediante la combinación de recursos en locaciones físicas diferentes, o mediante la simplificación del sistema de control [1, 8, 10, 11, 15].

5.1 Justificación del uso de Virtualización

Debido al crecimiento vertiginoso de las tecnologías de la información en el campo de los sistemas distribuidos, las redes tradicionales han logrado alcanzar un nivel transaccional que antes no era posible. En muchas organizaciones tanto el almacenamiento como la potencialidad de sus sistemas no son ´íntegramente aprovechados, derivando en lo que se conoce como deslocalización (granja de servidores desaprovechados) con un sistema por cada servidor, es aquí donde la virtualización tiene una participación muy importante, permitiendo incrementar el uso de cada dispositivo y decrementan los costos reutilizando el mismo hardware [9, 15].

Existen diversos enfoques de virtualización, aquí listaremos algunos de ellos [8, 9, 15]:

- **Emulación o simulación:** la máquina virtual simula un hardware completo, admitiendo un sistema operativo guest (invitado) completamente diferente. Este enfoque fue muy utilizado para permitir la creación de software para nuevos procesadores antes que estuvieran físicamente disponibles [1].
- **Virtualización nativa y virtualización completa:** la máquina virtual simula un hardware suficiente para permitir un sistema operativo “guest” sin modificar (uno diseñado para la misma CPU) para correr de forma aislada. Típicamente, muchas instancias pueden correr al mismo tiempo.
- **Virtualización parcial (y se incluye la llamada “virtualización del espacio de direcciones”):** la máquina virtual simula múltiples instancias entornos subyacentes del hardware, particularmente “el espacio de direcciones”. Este entorno admite compartir recursos y aislar procesos, pero no permite instancias separadas de sistemas operativos “guest”.

- **Paravirtualización:** la máquina virtual no necesariamente simula un hardware, en cambio ofrece una API especial que sólo puede usarse mediante la modificación del sistema operativo “guest” [1].
- **Virtualización a nivel del sistema operativo:** virtualizar un servidor físico a nivel del sistema operativo permitiendo múltiples servidores virtuales aislados y seguros correr en un solo servidor físico. El entorno del sistema operativo “guest” comparte el mismo sistema operativo que el del sistema “host” (el mismo kernel del sistema operativo es usado para implementar el entorno del “guest”). Las aplicaciones que corren en un entorno “guest” dado lo ven como un sistema autónomo [8, 11].
- **Virtualización de aplicaciones:** consiste en el hecho de correr una aplicación de escritorio o de servidor, usando los recursos locales, en una máquina virtual apropiada. Esto contrasta con correr la aplicación como un software local convencional (software que fueron “instalados” en el sistema), tales aplicaciones virtuales corren en un pequeño entorno virtual que contienen los componentes necesarios para ejecutarse como: entradas de registros, archivos, variables de entorno, elementos de uso de interfaces y objetos globales. El mencionado entorno virtual actúa como una capa entre la aplicación y el sistema operativo, eliminando los conflictos entre aplicaciones y entre las aplicaciones y el sistema operativo [8, 11].
- **Máquina virtual basada en el núcleo:** es una solución para implementar virtualización completa con Linux sobre hardware x86. Está formada por un módulo del núcleo (con el nombre kvm.ko) y herramientas en el espacio de usuario, siendo en su totalidad software libre. El componente KVM14 para el núcleo está incluido en Linux desde la versión 2.6.20 [8, 11].

5.2 Ventajas de la Virtualización

Las principales ventajas de las Honeynets virtuales son la gran reducción en los costos y la facilidad del mantenimiento de toda la infraestructura, esto se debe a que todo está integrado en un único sistema, y a que es absolutamente factible diseñar y poner en funcionamiento una Honeynet como la que hemos visto anteriormente. Dado que las máquinas virtuales suelen encapsularse en archivos, se obtiene una importante flexibilidad en los despliegues, ya que el salvado, copia o eliminación de los archivos con las imágenes virtuales es rápida, cómoda y sencilla. Como así también, la posibilidad de recrear diferentes infraestructuras de red en poco tiempo y de una manera

simple. Luego, se deducen dos importantes ventajas: flexibilidad y escaso o tiempo nulo de recuperación ante un incidente [8, 10].

Por otro lado, las máquinas virtuales pueden contener sistemas de distinta índole: es absolutamente posible tener un servidor de virtualización, coexistiendo con diferentes tipos de software, como ser: Windows, Linux, BSD, Solaris, etc., por ejemplo, todo ello en una ´única máquina física sustituyendo de esta manera enormes conjuntos de sistemas que apenas se usan, por unos cuantos mejor utilizados. De aquí se emanan otras dos ventajas: bajo costo y ´óptimo aprovechamiento de los recursos [4, 8, 10, 15].

Una gran ventaja a tener en cuenta es la simplificación de la administración, porque separa los núcleos con una aplicación ejecutándose en cada uno, aumentando así la seguridad y facilidad de gestión. Además de reducir el hardware, logrando que los espacios ocupados por el equipamiento tiendan a reducirse considerablemente [4, 8, 10, 15].

La disociación entre lo físico y lo virtual permite obtener otras ventajas, la principal es la seguridad, ya que las máquinas virtuales sólo pueden comunicarse con otras máquinas virtuales y con el exterior a través de conexiones correctamente configuradas [4, 8, 10, 15].

e. Materiales y Métodos

1. Métodos

Partiendo de que el objetivo de la investigación científica es llegar al conocimiento científico de la realidad que se estudia, a través de la metodología la cual se basa en un conjunto de métodos y técnicas que forman la teoría y la práctica del conocimiento; el desarrollo del presente proyecto se enmarca en el método inductivo, el método deductivo y la utilización de técnicas (lectura, entrevista, observación de campo, etc.).

Como en toda investigación se utilizó el **Método Científico**, el cual comprende el estudio sistemático de la naturaleza que incluye las técnicas de observación, reglas para el razonamiento y la predicción, ideas sobre la experimentación planificada y los modos de comunicar los resultados experimentales y teóricos.

El **Método Deductivo**, se aplicó en el proyecto al momento de realizar el estudio de la red actual de la UNL y sus puntos críticos hasta llegar al objetivo específico de poder realizar el diseño e implementación de una Honeynet.

Para el desarrollo del proyecto se aplicaron las siguientes etapas:

Análisis:

Es la fase principal del proyecto, ya que aquí se analizó la situación actual de la red de datos de la UNL para determinar sus puntos críticos los cuales sirvieron de referencia para determinar los ataques que sufre la red y de esta manera poder dar una solución a ellos mediante el desarrollo de este proyecto.

Se realizó una entrevista en el departamento de Telecomunicaciones (UTI) para poder determinar los siguientes puntos:

- Proveedor de internet
- Ancho de banda
- Equipo Hardware disponible
- Políticas o reglamento interno.
- Mecanismos de seguridad disponibles físicos y lógicos.

Desarrollo:

Es la ejecución total del proyecto, se realizó una revisión bibliográfica para poder determinar el tipo de Honeynet que será implementado en la red de datos de la UNL. Además se realizó la selección de los equipos, las herramientas y la técnica de implementación de la Honeynet. Para ello se realizó lo siguiente:

a) Revisión Bibliográfica de conceptualización de Honeynet.
b) Recopilación de Casos de éxito de implementación de Honeynet en instituciones de educación superior.
c) En base a los recursos disponibles seleccionar el tipo de Honeynet y la técnica adecuada para su implementación.
d) En este proyecto se determinó implementar una Honeynet Virtual de Generación III Autocontenida.

Implementación:

Básicamente se realizó el levantamiento de la Honeynet. Se realizaron todas las configuraciones necesarias para obtener el máximo rendimiento de la red y obtener resultados positivos en cuanto al enfoque de seguridad, es decir, reducir los ataques que sufre la red de datos de la UNL. Esto se logró mediante las siguientes actividades:

a) Seleccionar el equipo hardware para la implementación de la Honeynet.
b) Instalar el software en el host anfitrión (Centos 7 versión Servidor).
c) Instalar el software de virtualización en el host anfitrión (Virtual Box).
d) Instalar las máquinas virtuales, que son los elementos de la Honeynet.
    - Honeypot con sistema operativo Centos 7.
    - Honeywall con Honeywall CDROM.

Pruebas y Resultados:

Se realizó la etapa de pruebas de la Honeynet, con lo cual se pudo validar la funcionalidad de la misma. Se realizó un análisis estadístico para determinar el grado de seguridad que brinda la Honeynet y obtener una evaluación real de la misma. En esta fase se realizaron las siguientes actividades:

a) Configurar los elementos de la Honeynet con los parámetros de red establecidos.
b) Comprobar conectividad entre los elementos internos de la Honeynet.
c) Levantar los servicios que ofrecen el Honeypot, DHCP, HTTP, FTP y SSH.

d) Instalar la herramienta SEC (correlación de eventos), para monitorear la red y el funcionamiento de la Honeynet en tiempo real.
e) Validar la información obtenida por el funcionamiento de la Honeynet.

El **Método Inductivo**, fue utilizado a partir de la causa encontrada en el método deductivo; con la finalidad de hacer una revisión total de las particularidades hacia la generalidad del proyecto. Ya que todo proyecto de esta clase recae en el ambiente tecnológico y que se apoya en variables de tipo social, económicas, académicas, etc. Mismas que interactúan entre ellas en tiempo y espacio.

2. Técnicas

Para la recopilación de la información se utilizaron las siguientes técnicas:

La lectura, será utilizada para obtener conocimientos sobre el problema tratado, sirve como fundamentación teórica y poder sacar alguna conclusión importante del problema.

Entrevista, para la recopilación de información de la situación actual de la red de datos de la UNL, además utilizada como base para realizar la documentación del presente proyecto.

Observación Científica, técnica utilizada fundamentalmente para obtener información primaria acerca de los fenómenos que se investiga y para comprobar los planteamientos formulados en el proyecto.

f. Resultados

1 Fase 1: Describir la situación actual de la infraestructura de la red de datos de la UNL, para determinar sus puntos críticos

La Universidad Nacional de Loja, cuenta con una red de datos que une todos sus campus universitarios (Campus Central, Área de la Salud, Extensión Motupe, Punzara e Instituto de Idiomas). El proveedor de Servicios de Internet (ISP) es CEDIA, actualmente tiene 100 Mbps, de ancho de banda contratado. Ver Anexo 1, Unidad de Contratación Pública.

La Red Académica Avanzada del Ecuador (Red CEDIA) opera sobre la Red Nacional de TELCONET, uniendo las principales universidades, escuelas politécnicas, organizaciones de ciencia y tecnología del país, con plataformas de fibra óptica [16].

Es importante destacar que CEDIA forma parte de CLARA - Cooperación Latinoamericana de Redes Avanzadas, está constituida por redes de Latinoamérica.

1.1 Red académica (Red Avanzada)

Para su cumplimiento, CEDIA tiene los siguientes objetivos específicos [17-19]:

- Promover la creación de una red de telecomunicaciones con capacidades avanzadas.
- Fomentar y coordinar proyectos de investigación para el desarrollo de aplicaciones de tecnología avanzada de redes de telecomunicaciones y cómputo, enfocadas al desarrollo científico y educativo de la sociedad ecuatoriana.
- Promover el desarrollo de acciones encaminadas a la formación de recursos humanos capacitados en el uso de aplicaciones educativas y de tecnología avanzada de redes de telecomunicaciones y cómputo.

Características:

- Red de alta velocidad.
- Red sin congestión.
- Anillo Nacional EC de 1 Gbps.

1.2 Centro de Cómputo de la Universidad Nacional de Loja

Un centro de cómputo representa una entidad dentro de la organización, la cual tiene como objetivo satisfacer las necesidades de información de la empresa, de manera veraz y oportuna. Su función primordial es apoyar la labor administrativa para hacerla más segura, fluida y así simplificarla. Es responsable de centralizar, custodiar y procesar la mayoría de los datos con los que opera la organización [20].

Prácticamente todas las actividades de los demás departamentos se basan en la información que les proporciona dicho centro. La toma de decisiones depende en gran medida de la capacidad de respuesta del proceso de datos. Por lo anterior, casi no se escatima la inversión para proveerlo del equipo técnico (material y humano) necesario [20].

1.2.1 Objetivo del Centro de Cómputo

El principal objetivo es el de concentrar el procesamiento de datos e información de una manera sistematizada y automática [20].

1.2.2 Organigrama

En la Universidad Nacional de Loja se esquematizan los siguientes recursos del centro de cómputo:

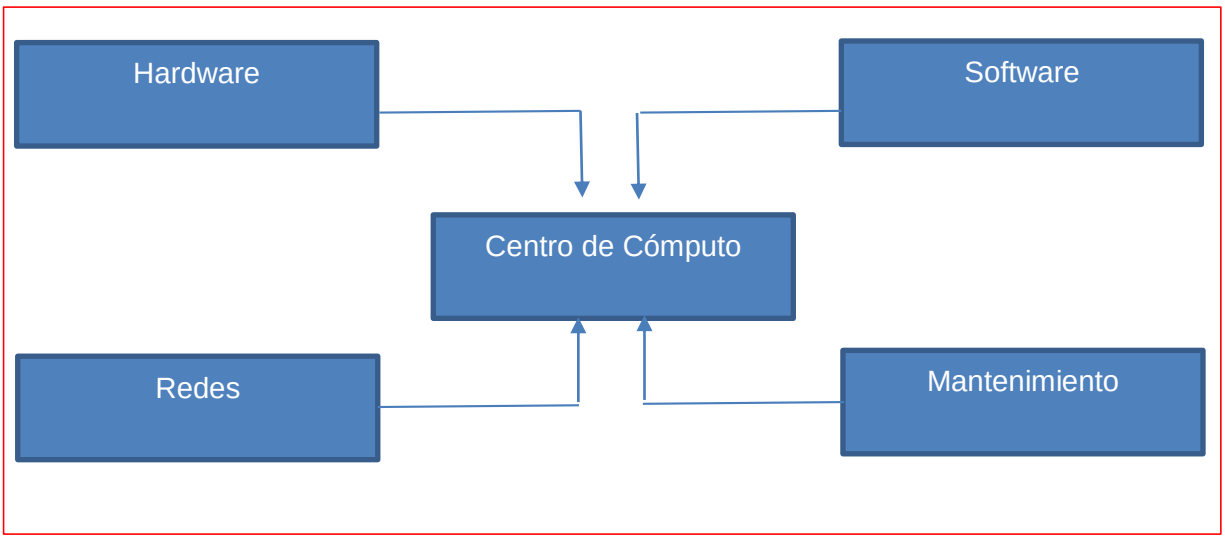


Figura 6: Recursos del Centro de Cómputo

1.3 Políticas de la Unidad de Telecomunicaciones e Información

El presente documento define el conjunto de Políticas de la Unidad de Telecomunicaciones e Información de la Universidad Nacional de Loja, que regirán durante el presente período [21].

Las políticas presentadas en este documento se enmarcan dentro de la reglamentación establecida por la Institución, que respecto de estas áreas considera:

- La Unidad de Telecomunicaciones e Información se define como el área de servicios que tiene como clientes todas las áreas de nuestra Universidad Nacional de Loja e incluyendo la MED.
- La Unidad de Telecomunicaciones e Información deberá cautelar los bienes muebles e inmuebles de la Universidad que le sean de su competencia, dentro de los cuales se consideran los datos e información que le sean confiados para su protección, administración, operación, revisión, adaptación y en general, toda acción relacionada con las funciones que al departamento sean de su competencia.

Las políticas institucionales de seguridad informática están basadas en lo establecido en la "Norma ISO/IEC 17799:2000 la cual es un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información", dicha norma ofrece recomendaciones en la gestión de la seguridad de la información, y define la Seguridad de la Información como la preservación de la confidencialidad, integridad y disponibilidad. A continuación se definen dichos conceptos:

- Confidencialidad: aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.
- Integridad: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
- Disponibilidad: aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Alcances

La aplicabilidad de estas políticas rige para la Universidad Nacional de Loja en su totalidad y conjunto. Los sistemas, equipos, software, líneas telefónicas y enlaces de comunicación adquiridos o contratados con cualquier finalidad por las diferentes áreas

y departamentos, con anterioridad a la fecha de emisión de estas políticas, quedarán igualmente sujetos a ellas y a las auditorías que pudieran realizarse bajo su amparo.

1.3.1 Políticas Generales

Aquí se detallan a continuación las políticas generales que se manejan actualmente en el departamento de Telecomunicaciones e Información (UTI):

- Políticas de definición
- Políticas de prestación de servicios
- Políticas de administración de recursos
- Política de coordinación de actividades
- Políticas de cobertura de los servicios
- Políticas de Salvaguarda y Confidencialidad
- Políticas de Protección de datos y sistemas
- Políticas de documentación digital o Impresa}

A continuación se detallan las políticas relacionadas con la seguridad informática y con la parte de redes.

1.3.1.1 Políticas de Prestación de Servicios

Los servicios que la Unidad de Telecomunicaciones e Información en sus diferentes secciones son: Mantenimiento Electrónico, Redes y Equipos Informáticos, Telecomunicaciones y Desarrollo de Software.

Los servicios prestados deben, para todos los casos, poseer una métrica de calidad, mediante la cual se midan: tiempos de respuesta, calidades de solución, calidades de satisfacción usuaria, entre otras variables.

La prestación de servicios de las secciones de la Unidad de Telecomunicaciones e Información debe, en todo momento, estar dotado de trazabilidad de procedimientos. Lo anterior implica procesos formales de solicitud de servicios, acción, respuesta y aceptación.

1.3.1.2 Políticas de Salvaguarda y de Confidencialidad

Los funcionarios de la UTI bajo cualquier forma de estructura, se comprometen a salvaguardar de todo riesgo y a guardar la más absoluta reserva y/o confidencialidad sobre toda la información, cualquiera sea su naturaleza, que bajo cualquier medio le sea entregada de parte de la Universidad Nacional de Loja, y que forme parte de los datos,

información, procedimientos, conocimientos, comportamientos, actividades, desempeños, funcionamientos, metodologías, rutinas, acciones y en general de toda expresión, en el medio que fuere, que pertenezca a la propiedad exclusiva de la Universidad Nacional de Loja.

Se incluye en este punto, toda información de tipo comercial, financiero, metodológicas, de procesos, de conocimientos propios y adquiridos, experimentales, ya sea su conocimiento de carácter privado o público y que pertenezca a la Universidad Nacional de Loja.

1.3.1.3 Políticas de Protección de datos y sistemas

El equipo computacional perteneciente a la Universidad Nacional de Loja estará bajo la exclusiva administración de la UTI y por lo tanto queda prohibido al usuario realizar intervenciones no debidas, entre las que se encuentran:

- Manipulación no autorizada.
- Apertura, reemplazo y/o desconexión de componentes.
- Reasignaciones permanentes o temporales sin autorización.
- Instalación de programas, sistemas, módulos y/o archivos externos.
- Empleo de juegos y/o programas con fines no laborales.
- Modifica la configuración de sistemas, programas o dispositivos.
- Desinstalar sistemas, programas, módulos oficiales de la Universidad Nacional de Loja.
- Conexión a redes eléctricas o de Datos no certificadas y o autorizadas

Respecto de lo definido con el fin de proteger las instalaciones, equipos, datos y sistemas de la acción de virus computacionales, será lo estipulado por la UTI lo que permanezca vigente y con prohibición para los usuarios el modificar y/o transgredir las disposiciones establecidas [21].

Para mayor conocimiento de cada una de las políticas se recomienda ver el Anexo 2: Políticas de la Unidad de Telecomunicaciones e Información.

1.4 Red de Datos de la Universidad Nacional de Loja

La red de datos de la UNL tiene su centro de cómputo en la UTI (Departamento de Telecomunicaciones e Información). Desde el cual se realiza el monitoreo y control de la misma.

La red tiene la siguiente estructura y distribución de equipos:

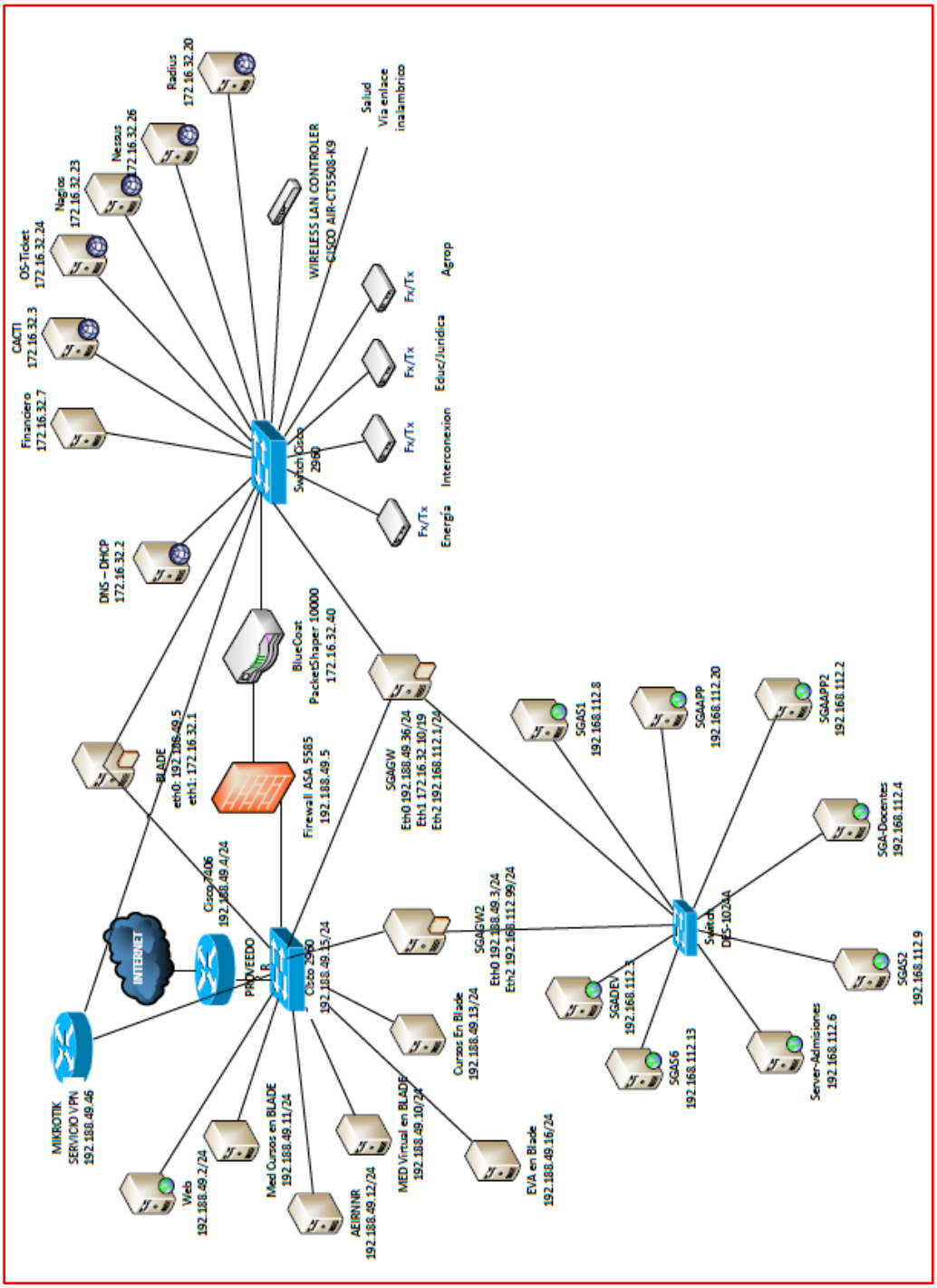


Figura 7: Ubicación de Equipos de la Red de Datos [21]

Dentro del equipo de red se detallan los siguientes:

TABLA I: HARDWARE DE RED [21]

Hardware de Red				
N°	**Equipo**	**Características**	**Función**	**Seguridad**
1	Router Mikrotik	Router para realizar implementación de servicios VPN (Red Privada Virtual).	Realizar VPN (Red Privada Virtual) para el Administrador.	Control de Usuarios aplicando usuario y contraseña.
2	Router CISCO 7604	Cuatro ranuras (2 ranuras de supervisor y 2 ranuras de interfaz). Capacidad de protección procesador de ruta: 1 + 1	Cumple dos funciones enrutamiento y conmutación. En la función de enrutamiento logra la interconexión de redes y determina la mejor ruta para llegar a redes externas. En la función de conmutación, se encarga de la conversión (encapsulación) de señales de una interfaz a otra.	Desactivado Plug and Play. Cambiada la contraseña del Administrador. Desactivado broadcast SSID (Service Set Identifier)
3	Switch CISCO 2960	Dispositivo de interconexión utilizado para conectar equipos en la red interna.	Utilizado para distribuir internet a los servidores públicos.	Seguridad de Puertos.
4	Firewall ASA 5585		Protección de la red interna de la UNL.	Seguridad de puertos de acceso.

		Acceso remoto sumamente seguro.		
5	BlueCoat PacketShaper 10000	Reservar ancho de banda para aplicaciones críticas. Limitar el tráfico perjudicial y desacelerar los aumentos de ancho de banda.	Segmentar el ancho de banda a las diferentes áreas q compone la red de datos de la Universidad.	Protegida por el firewall.
6	Wireless LAN Controller CISCO AIR-CT5508-K9	Equipo de red que gestiona el direccionamiento IP y la señal de los AP (Acces Point).	Maneja toda la señal inalámbrica (WiFi) de la red de datos de la UNL.	Control de Acceso. Firewall CISCO. Protocolo de Seguridad SSH.
7	Servidor WEB	Servidor Público q contiene las distintas aplicaciones web q requieren los departamentos de la UNL.	Realizar peticiones y respuestas de los diferentes usuarios.	Implementado con el Sistema Operativo Windows Server. Firewall propio.
8	Servidor MED CURSOS	Servidor Público que registra toda la información de los cursos de modalidad a distancia de la UNL.	Realizar peticiones y respuestas de los diferentes usuarios.	Implementado con el Sistema Operativo Windows Server. Firewall propio
9	Servidor AEIRNNR (Área de Energía)	Servidor Público que maneja el portal de la MED.	Realizar peticiones y respuestas de los diferentes usuarios.	Implementado con el Sistema Operativo Windows Server.

				Firewall propio
10	Servidor EVA (Entorno virtual de Aprendizaje)	Servidor Virtualizado en el Blade, que controla los diferentes cursos del EVA, para los estudiantes de todas las carreras de la UNL.	Realizar peticiones y respuestas de los diferentes usuarios.	Implementado con el Sistema Operativo Windows Server. Firewall propio
11	SERVIDOR DNS - DHCP	Servidor Privado.	Virtualizado en el Blade, realiza la asignación de IP'S dinámicas.	Firewall CISCO ASA Firewall propio del equipo Control de acceso puerto-protocolo.
12	SERVIDOR Financiero	Servidor Privado.	Manejo y control del departamento financiero de la UNL.	Firewall CISCO ASA Firewall propio del equipo Control de acceso puerto-protocolo.
13	SERVIDOR NAGIOS	Servidor Privado.	Manejo de aplicación de tesistas, autenticación de usuarios.	Firewall CISCO ASA Firewall propio del equipo Control de acceso puerto-protocolo.
14	SERVIDOR RADIUS	Servidor Privado.	Manejo de aplicación de tesistas, atutenticación de usuarios de EDUROAM.	Firewall CISCO ASA Firewall propio del equipo Control de acceso puerto-protocolo.

15	SERVIDOR SGA (Sistema de Gestión Académica)	Varios servidores que distribuyen la carga de información.	Realizar consultas y respuestas de estudiantes y docentes.	Firewall CISCO ASA Firewall propio del equipo Control de acceso puerto-protocolo.

1.5 Seguridad en la Red de Datos de la Universidad Nacional de Loja

La seguridad de la red de datos de la UNL se preocupa principalmente de proteger la información tomando en cuenta los tres aspectos fundamentales que son: la confidencialidad, la integridad y la disponibilidad.

Para poder cubrir con estos aspectos importantes se aplican los dos tipos de seguridad informática q son la seguridad física y la lógica.

1.5.1 Seguridad Física

Es muy importante ser consciente que por más que nuestra red de datos sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc.; la seguridad de la misma será nula si no se ha previsto como combatir un incendio 22].

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático [22].

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial [22].

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo implementados para proteger el hardware y medios de almacenamiento de datos.

1.5.1.1 Tipos de Desastres

Cada sistema es único y por tanto la política de seguridad a implementar no será única. Es por ella que siempre se recomendarán pautas de aplicación general y no procedimientos específicos.

Las principales amenazas que se prevén en Seguridad Física son:

- Desastres naturales, incendios accidentales, tormentas e inundaciones.

- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.

A continuación se lista los peligros más importantes que se corren en un centro de cómputo; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos [21,22].

- Incendios
- Inundaciones
- Condiciones Climatológicas
- Señales de Radar
- Instalación Eléctrica
- Ergometría

En lo que respecta a la seguridad física actual de la red de datos (Centro de Cómputo) se detallan los siguientes:

- Restringir el acceso del personal no autorizado al centro de cómputo.
- Sistema de enfriamiento por aire acondicionado.
- Cableado estructurado con Cable UTP Cat. 5E.
- Se tiene dos UPS de 24 KVA que brindan 10 min de suministro de energía alterna.
- No se cuenta con un generador de energía.

1.5.2 Seguridad Lógica

La seguridad lógica consiste en la aplicación de barreras y procedimientos que respaldan el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo [22].

En el centro de datos de la UNL las medidas de seguridad lógica son las siguientes:

- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no corresponden.
- Asegurar que se estén utilizando los datos por las aplicaciones debidas.
- Verificar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Comprobar que la información recibida sea la misma que ha sido transmitida.

- Disponen de pasos alternativos de emergencia para la transmisión de información.
- La redundancia implica, necesariamente, duplicar infraestructura. Es por esta razón que aplica redundancia lógica, solamente en ciertos servidores (SGA). Con un tipo Activo – Activo (cuando funcionan simultáneamente varios servidores, con un mecanismo adicional de balanceo de carga) [23].

La información es el recurso más valioso de una organización, y se encuentra expuesta a actos intencionales como accidentales de violación de su confidencialidad, alteración, borrado y copia, por lo que se hace necesario que el departamento de telecomunicaciones adopte medidas de protección contra accesos no autorizados.

Los siguientes mecanismos de seguridad son los que se encuentran implementados actualmente en la red de datos de la UNL.

1.5.2.1 Clave de Autorización de Acceso

Las claves o contraseñas son la única identificación para el usuario, por esta razón deben ser difíciles de adivinar y deberán cambiarse con frecuencia.

Seguridad aplicada en el Router MikroTick, mediante este router se implementa una Red Privada Virtual (VPN), para realizar configuraciones de red.

1.5.2.2 Copias y Backup de Respaldo

Es importante mantener en lugar seguro y externo al sitio de trabajo, copias actualizadas de la información vital de cada dependencia, con el fin de garantizar la oportuna recuperación de datos y programas en caso de pérdidas o daños en los equipos.

El servidor de respaldos maneja las copias de seguridad de información de las configuraciones de los equipos.

1.5.2.3 Cortafuegos (Firewall Cisco ASA 5585)

Este mecanismo de seguridad ayuda a la universidad a encontrar un equilibrio entre seguridad y productividad [24].

Las ventajas que brinda este equipo para la seguridad de la red de datos de la UNL, se detallan las siguientes [24]:

- Visibilidad y control de aplicaciones y microaplicaciones, con controles basados en el comportamiento.

- Seguridad online robusta
- Protección avanzada contra amenazas con un sistema de prevención contra intrusiones (IPS) completo y de gran efectividad.
- Acceso remoto sumamente seguro.
- Protección contra botnets.
- Protección contra amenazas procedentes de Internet.

1.5.2.4 Seguridad de los Servidores del SGA (Sistema de Gestión Académica)

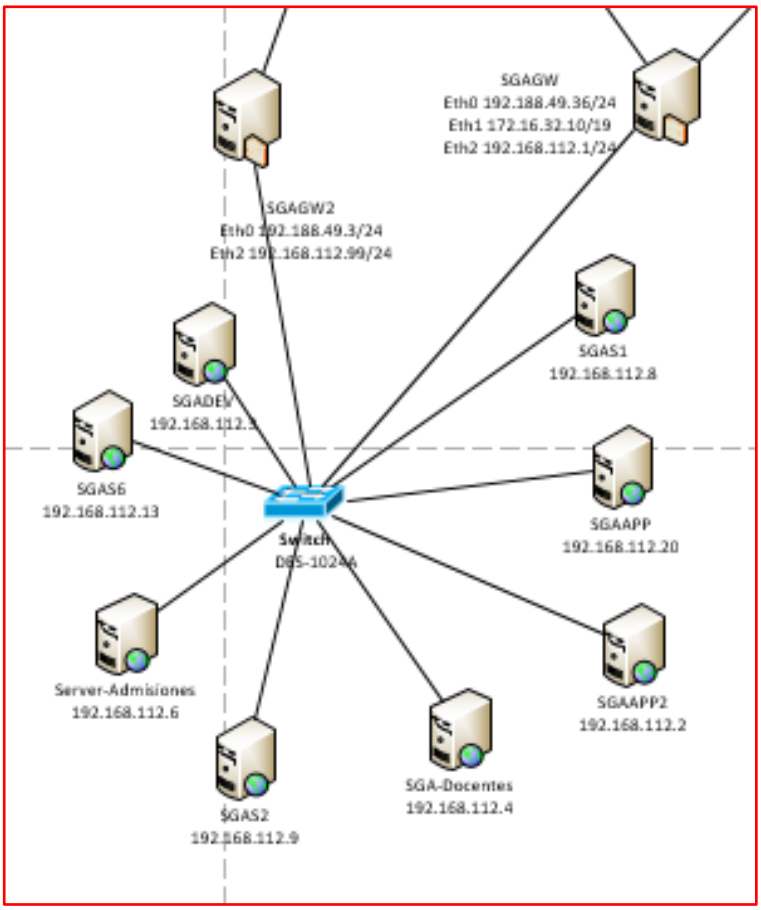


Figura 8: Servidores del SGA [21]

Toda la información que corresponde al SGA circula por los ocho servidores, en los cuales se nivelan la carga o flujo de datos [21].

EL SGA se encuentra divido en tres ramas importantes:

- Docentes
- Estudiantes
- Administración

En la rama de los Docentes se maneja todo lo correspondiente a listado de docentes y registro de calificaciones. Es decir existe permiso de lectura y escritura para los docentes.

En la rama de los Estudiantes, se controla el acceso a las calificaciones de cada uno de ellos y se gestiona las matrículas conjuntamente con los pagos que se realizan en el banco. Ya que tiene integrado un módulo que lo gestiona el Banco de Loja.

Dentro de la rama de Administración, se controla el acceso, es decir identificar los usuarios (docentes, estudiante y administrativos) y sus peticiones.

Las secretarias de las diferentes carreras tienen acceso únicamente a los datos de los estudiantes, para emitir reportes.

Los coordinadores de carrera tienen acceso más amplio, ya que son los que ingresan la malla curricular de la carrera correspondiente, asignación de docentes a unidades y reportes de los estudiantes.

El servidor público es el encargado de identificar la petición que realiza el usuario para emitir la respuesta según corresponda. Este servidor tiene como mecanismo de seguridad IP tables y un firewall propio. Es decir, tiene un nivel de seguridad medio.

En cada una de las tres ramas se maneja la identificación de usuarios mediante un web service para autenticación.

Dentro de la seguridad se maneja la encriptación de datos en los docentes y administradores, en estudiantes no aplica debido a que las secretarias deben tener acceso libre a los datos de los mismos [21].

El SGA maneja solamente una base de datos en Posgress, mediante un acceso local creando credenciales IP para los administradores. Utiliza webservice para realizar autenticación en diferentes proyectos de tesis [21].

1.6 Buenas Prácticas para el control de Seguridad

Se detallan buenas prácticas que incluyen un total de 20 puntos de control de seguridad a tener en cuenta para protegernos de posibles ataques tanto externos como internos.

- Inventario de dispositivos autorizados y no autorizados.
- Inventario de software autorizado y no autorizado.

- Configuraciones seguras de hardware y software para portátiles, equipos y servidores.
- Configuraciones seguras para dispositivos de red (Firewalls, Routers y Switches).
- Defensa perimetral. Establecer una buena seguridad “perimetral” mediante proxys, redes DMZ, sistemas de prevención de intrusiones (IPS – Intrusion Prevention System), firewalls… Para ataques que provengan del exterior, esta es la primera puerta que se encontrarán nuestros amigos los “malos”, por lo que conviene tenerla con unas cuantas cerraduras.
- Mantenimiento, monitorización y análisis de registros de auditoría.
- Seguridad en aplicaciones software.
- Uso controlado de privilegios de administración.
- Acceso controlado a recursos basado en su grado de confidencialidad.
- Análisis de vulnerabilidades y sus correspondientes mitigaciones.
- Control y monitorización de cuentas.
- Defensa frente a malware.
- Control y limitación de puertos de red, protocolos y servicios.
- Control de dispositivos wireless.
- Prevención de fugas de información.
- Ingeniería de red segura.
- Test de intrusión y pruebas por parte de equipos “Red Team”.
- Capacidad de respuesta frente a incidentes.
- Capacidad de recuperación de datos.
- Estudio de técnicas de seguridad y formación necesaria para cubrir huecos.

2 Fase 2: Selección del Tipo y la Técnica de Implementación de la Honeynet en la red de datos de la UNL

Después de haber realizado el análisis de toda la recopilación bibliográfica sobre la arquitectura y el tipo de Honeynet; se detalla a continuación una comparación sistemática entre los tipos de Honeynet y la justificación de la selección de la técnica de implementación.

El primer aspecto que se debe definir y tener claro es el concepto de Honeynet, la cual nos permite estar un paso adelante que el enemigo, permitiendo aprender de las amenazas y del comportamiento de los atacantes, para implementar una arquitectura de seguridad proactiva que no solo permita defenderse de tales amenazas, sino también someterlas antes de que sucedan [25].

Una Honeynet básicamente es un Honeypot de alta interacción que consta de una red de sistemas, cuyo propósito es ser comprometida por un usuario malicioso, con la finalidad de aprender sobre las herramientas, tácticas y motivos que alientan a este tipo de usuarios [26].

Esta red captura y controla mediante un firewall todo el tráfico destinado a los equipos dentro de ella para su posterior análisis.

Existen tipos de Honeypots basados en el nivel de interacción que tendrá el atacante con el Honeypot.

Para el desarrollo del presente proyecto fin de carrera se ha seleccionado el **Honeypot de Investigación**, ya que su propósito es ser atacado y servir como herramienta didáctica para aprender a proteger los sistemas contra nuevas amenazas. Es principalmente usado para investigación en instituciones como Universidades, organizaciones gubernamentales, militares. En otras palabras, el Honeypot de Investigación cumple la función de capturar información para ser analizada [25,27].

Además se usan para recolectar información sobre los movimientos de los intrusos, es decir, se registra cada movimiento del atacante para usar esta información y crear perfiles de los mismos.

Existe otra clasificación que divide ambos tipos de Honeypots, que se basa en el grado en el que se compromete o arriesga a la red real:

Se ha seleccionado el **Honeypot de baja interacción**, porque emulan servicios, su instalación es del tipo “plug and play”, al emular servicios constituyen un sistema controlado por consiguiente el riesgo inmerso es limitado.

Los servicios no son reales y no representan un riesgo como tal por su capacidad limitada [25, 27, 28].

2.1 Arquitectura de la Honeynet

La arquitectura de la Honeynet es única y se basa en tres puntos importantes, control de datos, captura de datos y la recolección y análisis de datos. Los cuales se han definido conceptualmente a continuación.

Para mantener el ambiente controlado la clave en la arquitectura de la Honeynet es su Puerta de Salida (Gateway) llamado Honeywall. Este dispositivo separa la Honeynet del resto del mundo. Por el Honeywall atraviesa todo el tráfico desde y hacia la Honeynet [27,26].

El Honeywall es un dispositivo que originalmente era de Capa 3 pero actualmente puede ser un bridge invisible de Capa 2. Tiene tres interfaces de red (eth0, eth1, eth2); las dos primeras (eth0, eth1), como puertas de entrada y salida, forman el bridge de Capa 2 separando la Honeynet con el mundo, y una tercera interface de red opcional que sirve para administración.

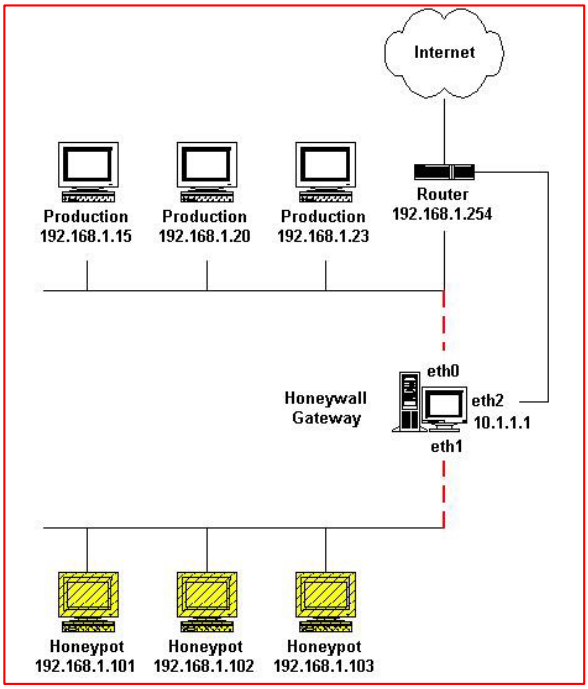


Figura 9: Arquitectura de una Honeynet [26]

Para crear una arquitectura correctamente se ha definido unos requisitos que garantizarán el correcto funcionamiento de la Honeynet y mantener un ambiente seguro para los sistemas contiguos a la red.

Estos requisitos son: control de datos, captura de datos y recolección de datos.

2.1.1 Control de Datos

El control de datos en una Honeynet se encarga de mitigar o de bloquear todo riesgo que se produzca desde los Honeypots hacia el mundo.

Recordar que en la Honeynet se usan sistemas no emulados, lo cual eleva el riego de ser usado como herramienta de ataque. Se debe definir qué nivel de riesgo se va manejar en la Honeynet, entre mayor sea el riesgo, mayor será la cantidad de datos obtenidos del atacante porque está aumentando la libertad con la que él puede interactuar con los sistemas.

El Control de Datos es el requerimiento más importante en una Honeynet y es imprescindible que por ningún motivo se deje abierto el acceso directo sin restricciones desde y hacia los Honeypots en una Honeynet.

En otras palabras el control de datos debe actuar de manera 'fail-close', lo que significa que si este falla por cualquier motivo inclusive el de ser blanco de un ataque, al caer el sistema de control de datos la Honeynet quede totalmente bloqueada de la red.

La implementación del control de datos debe ser la suma de diferentes mecanismos sobrepuestos como capas para evitar un punto único de fallo. Dependiendo de los tipos de Honeynet pueden ser: Gateway IDS, restricciones en consumo de ancho de banda, contador de conexiones. A medida que las generaciones de Honeynet vayan madurando se desarrollarán nuevas técnicas de bloqueo [26, 29, 30].

2.1.2 Captura de Datos

La captura de datos consiste en el monitoreo y registro de toda la actividad de los atacantes con los Honeypots. Al igual que el control de datos, la captura debe ser implementada en capas, proporcionando varios niveles y tipos de captura. Distintos mecanismos de captura deben agruparse, proporcionando una mayor gama de tipo de datos capturados y previniendo también los puntos únicos de fallo. Estos mecanismos pueden ir desde un simple sniffer que registre todos los datos que pasan por la red,

hasta un complejo sistema que permita registrar datos sobre canales encriptados como IPSec, SSH, SSL.

Dentro de la captura de datos se debe analizar el lugar para almacenar la información recolectada, la cual no debe grabarse en forma local sino debe ser registrada y almacenada en un sistema seguro separado de los Honeypots [26, 29,30].

2.1.3 Recolección y Análisis de Datos

La recolección de datos está planteada para el caso en que se tengan varias Honeynets en un entorno distribuido. Puede ser a nivel nacional o en varios sectores centralizando los datos recogidos.

El análisis es el punto en el que los datos recogidos por la Honeynet son analizados y estudiados en busca de patrones de ataque, ataques nuevos y lo que se haya definido como objeto de investigación [26, 29, 30].

2.2 Tipos de Honeynet

Para definir el tipo de Honeynet se ha realizado un análisis sistemático de cada tipo, se detalla a continuación:

TABLA II: TIPOS DE HONEYNET [26]

	Tipos de Honeynet		
	Honeynet de Generación I	**Honeynet de Generación II**	**Honeynet de Generación III**
Origen	Fue la primera arquitectura desarrollada la Honeynet Project en 1999 y se mantuvo hasta finales del año 2001.	Este segundo modelo dentro de las generaciones de las Honeynets fue lanzado y ha sido usado desde principios del 2002 por el Honeynet Project.	Esta arquitectura se dio a conocer a inicios del 2005. Con respecto a su antecesora muy similar, ya que mantiene los mismos dispositivos y características.

Arquitectura	Se compone de una máquina Gateway (llamada firewall) responsable del control de datos y otra denominada (IDS: Intrusion Detection System / Sistema de detección de intrusos) que es responsable de la captura de datos.	Aumentar la interacción con el atacante para aumentar la cantidad y calidad de datos recolectados.	Mantiene los mismos dispositivos y características. Mejora las versiones de las herramientas usadas y su principal objetivo es analizar los datos recogidos
Características	La máquina firewall dispone de 3 interfaces de red (interna, externa y administración) , la interfaz externa es usada para conectarse a Internet, la interfaz interna para conectarse a la Honeynet y la última para	Las tareas de control y captura de datos ahora están centralizadas en un solo dispositivo llamado Honeywall lo que permite que esta arquitectura sea fácil de desarrollar y mantener	unifica todos los datos registrados por cada herramienta de la captura de datos relacionándolos con los datos proporcionados por el control de datos, de esta forma podemos saber precisamente qué conexión generó una alerta y seremos capaces

	conectarse con el servidor de logs 4, todas las conexiones desde y para la Honeynet pasan a través de esta máquina Gateway		de rastrear todos los paquetes que están relacionados a esa conexión

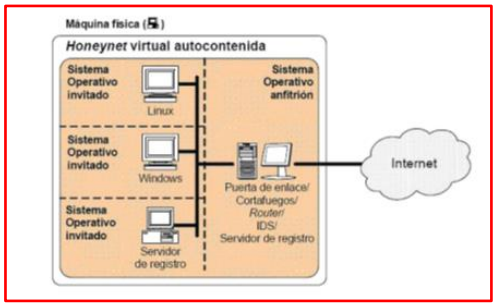
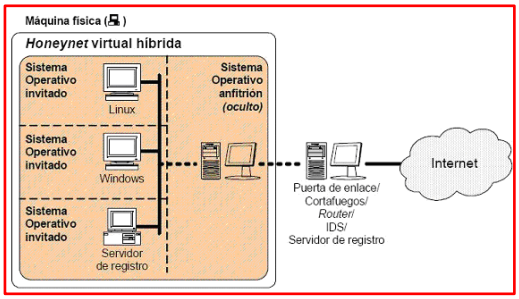
2.2.1 Honeynet Virtual

Una Honeynet Virtual se basa en el mismo concepto de la Honeynet pero implementándose dentro de un mismo computador, todos sus dispositivos son virtualizados mediante un software que permita esta tecnología [26, 29, 30].

Dentro de una máquina física se levantan los Honeypots como máquinas virtuales formando la Honeynet Virtual. Dependiendo de la configuración de cada uno, y de la arquitectura de red, podríamos hablar de Honeynets virtuales de I, II, III generación.

Las Honeynet Virtuales se dividen en dos grandes tipos: AutoContenidas e Híbridas [26, 29, 30].

TABLA III: TIPOS DE HONEYNET VIRTUALES [26]

Tipos de Honeynet Virtual	
Honeynet Virtual Autocontenida	**Honeynet Virtual Híbrida**
Engloba a una Honeynet en un solo equipo. La red entera está virtualmente contenida en un único y físico sistema. Una red Honeynet típicamente consiste de un cortafuego para Control de Datos y Captura de Datos, y los Honeypots dentro de la Honeynet.	Combina una Honeynet Clásica con una Honeynet Virtual, se agrega un dispositivo adicional en la arquitectura. Uno sirve como Honeywall (punto de entrada, control y recolección de información de la Honeynet) y otro levanta la red virtual de Honeypots
 Figura 10: Esquema de Honeynet Virtual Autocontenida [8].	 Figura 11: Esquema de Honeynet Virtual Híbrida [4].

2.3 Virtualización

Debido al crecimiento vertiginoso de las tecnologías de la información en el campo de los sistemas distribuidos, las redes tradicionales han logrado alcanzar un nivel transaccional que antes no era posible. En muchas organizaciones tanto el almacenamiento como la potencialidad de sus sistemas no son íntegramente aprovechados, derivando en lo que se conoce como deslocalización (granja de servidores desaprovechados) con un sistema por cada servidor, es aquí donde la virtualización tiene una participación muy importante, permitiendo incrementar el uso de cada dispositivo y reduciendo los costos reutilizando el mismo hardware [29, 31].

2.3.1 Justificación del uso de Virtualización

La idea de virtualizar el sistema es reducir costos por requerimiento de dispositivos, entre más grande es la Honeynet, más dispositivos y espacio físico se necesita. En una Honeynet Virtual todo se encuentra en una sola máquina física. En el caso de aumentar más dispositivos virtuales simplemente se mejora el hardware de la máquina anfitriona.

Entre las limitaciones tenemos: el hardware necesario de la máquina que alberga a la Honeynet, el software que es usado para virtualizar, si el atacante toma en su poder la máquina anfitriona tendría control sobre toda la Honeynet y sería un peligro para los sistemas reales.

La disociación entre lo físico y lo virtual permite obtener otras ventajas, la principal es la seguridad, ya que las máquinas virtuales sólo pueden comunicarse con otras máquinas virtuales y con el exterior a través de conexiones correctamente configuradas [26, 30, 31].

2.4 Conclusión

Después de haber realizado un análisis sistemático de la situación actual de la red de datos de la Universidad Nacional de Loja y haber recopilado la información correspondiente se concluye de la siguiente manera:

Implementar una Honeynet Virtual de Generación III Autocontenida.

Requerimientos de Software

El sistema operativo que requiere el host anfitrión es:

- Sistema Operativo Linux: Centos 7 edición de Servidor.

El software requerido para la virtualización es:

- Virtual Box

El firewall utilizado por el proyecto Honeynet, denominado Honeywall es:

- Roo 1.4 basado en Centos

El programa para la captura de datos es:

- Sec

El sistema operativo requerido por el Honeypot es:

- Sistema Operativo Linux: Centos 7 edición de Servidor.

3 Fase 3: Diseño de la Honeynet

El análisis de los ataques en la red de datos de la UNL, se va a realizar mediante la implementación de una Honeynet Virtual. Se va a diseñar una Honeynet utilizando el software comercial de virtualización Virtual Box, programa con un excelente entorno de desarrollo para tecnologías Honeynet.

En este proyecto, se va a implementar una red Honeynet Virtual Gen III (3ra. Generación) que posea un solo Honeypot. La figura 11 muestra el diseño general de la Honeynet, en el cual se puede observar a la red Honeynet conectada y funcionando dentro de la misma red de producción.

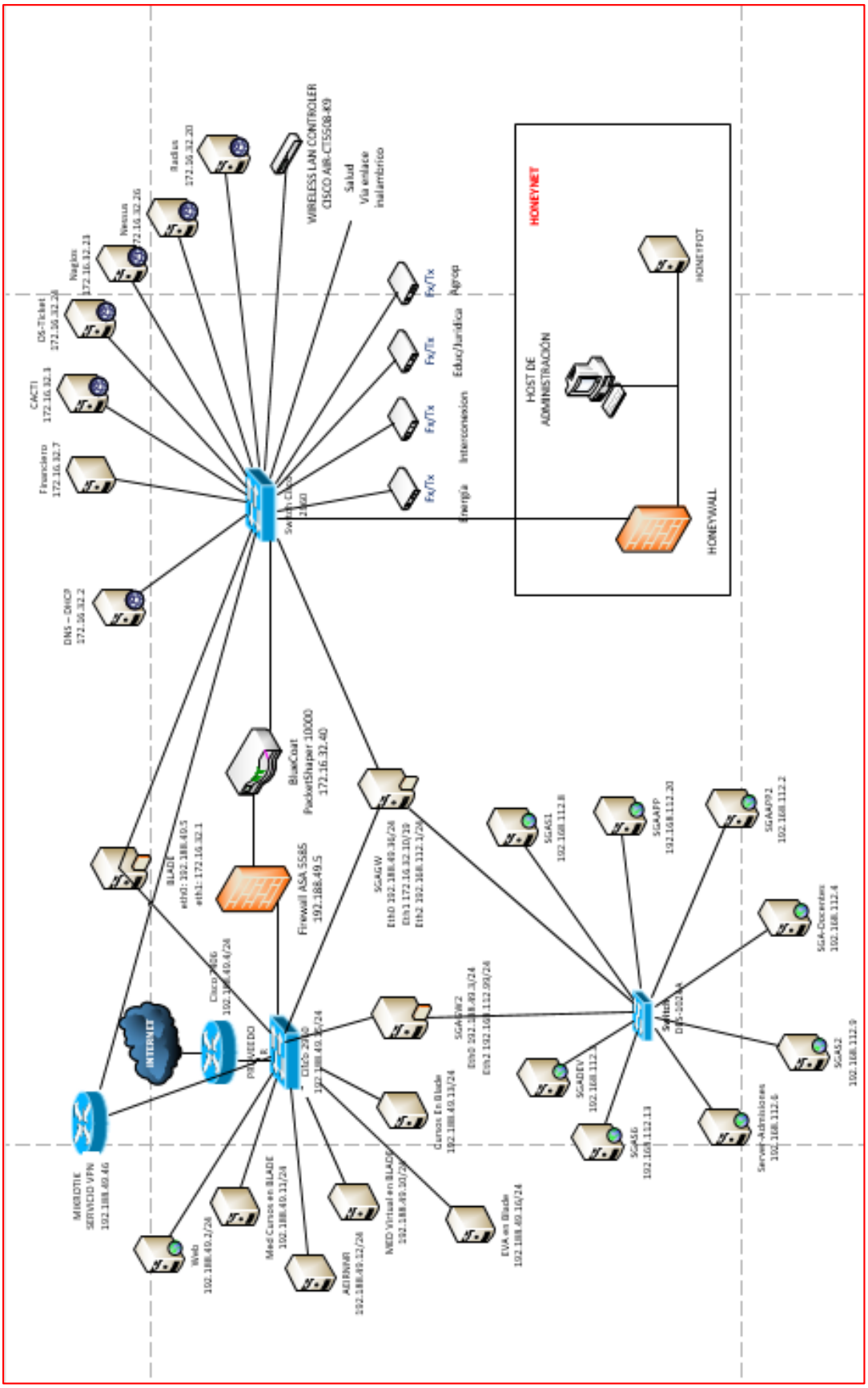


Figura 12: Diseño General de la Honeynet

3.1 Topología de Red a Utilizarse

Para la red Honeynet a implementarse en la red de datos de la UNL, se ha seleccionado la arquitectura de Honeynet Virtual Autocontenida, empleando virtualización y que para desarrollarla solamente es necesario un host físico en el cual se levantarán como máquinas virtuales a todos los elementos que conforman la Honeynet.

En la Figura 11 se puede observar los elementos de la Honeynet que serán equipos virtuales, ubicados dentro del recuadro amarillo que representa al único equipo físico empleado. Entonces se muestra la máquina física que usa una aplicación de virtualización para levantar las 3 máquinas virtuales, donde una corresponde al Honeywall, la siguiente al Honeypot y la tercera es el host de administración denominado “Walleye” en el proyecto Honeynet.

3.2 Software para la Virtualización

Es un sistema de virtualización por software libre propiedad de la empresa Sun Microsystems con licencia GPL disponible para todas las plataformas. VirtualBox tiene varias ventajas fundamentales:

- Funciona de manera realmente ligera: consume pocos recursos, las máquinas se ejecutan muy rápidas y funciona mejor en dispositivos portátiles
- Soporta sin problemas casi cualquier sistema operativo (cualquier Linux, Windows 7, Windows Server 2008 R2).
- Compartir archivos.
- Escritorio Remoto: la capa de abstracción de la interfaz de VirtualBox está basada en el protocolo RDP15 de Microsoft por lo que se conecta a cualquier máquina virtual usando escritorio remoto aunque el sistema operativo huésped no lo soporte. Esta capa está antes, y por lo tanto cualquier sistema o ventana se verán en el cliente de escritorio remoto.
- Integración con el sistema: si lo pones en modo "seamless integration".
- Ofrece soporte para aceleración 3D en las máquinas virtuales, así que funciona la interfaz 3D Aero en Vista/Windows 7 virtualizados.
- Soporte de USB dinámicamente, para añadir y detectar dispositivos USB.
- Son recomendables para sistemas operativos de 64 bits.

3.3 Selección de los Sistemas Operativos

Los sistemas operativos elegidos se basan en Linux, por ser software libre de código abierto y con ventajas notables respecto a los demás SO, en cuanto a estabilidad, velocidad y confiabilidad. Además de ser menos propenso a ataques de virus y malware.

Entonces para el SO del host anfitrión, se va a emplear la versión servidor de Centos 7 por su estabilidad, y dado que Centos es la versión de prueba del Red Hat (uno de los SO Linux más estables).

Así también, para el Honeypot (host virtual) se ha concluido emplear la distribución Centos versión Servidor 7. Debido a que en dichos hosts se va a configurar los diferentes servicios que brinde la red Honeynet. En tanto que para el Honeywall se emplea como SO el Honeywall CDROM.

3.4 Honeywall CDROM

Es un CD de arranque que contiene todas las herramientas necesarias para crear y utilizar una Honeynet Gateway (pasarela de red trampa). El CDROM está basado en una versión reducida de Linux Centos y está diseñado para ser utilizado como aplicación puesto que contiene sólo las herramientas necesarias para gestionar el Honeywall.

El Honeywall CDROM reduce muchos de los retos de implementar redes trampa al tiempo que crea una plataforma para tecnologías más avanzadas. Es un LiveCD de Linux muy reducido con funcionalidades muy específicas. Está diseñado para funcionar más como una aplicación que como un sistema operativo independiente. La pasarela creada por el CDROM incorpora sólo las herramientas necesarias para que ese sistema funcione. Este sistema ha sido elegido por su facilidad de implementación y configuración, además de ser una plataforma de seguridad de red flexible.

3.5 Centos Server 7 (Community ENTerprise Operating System)

Es una copia prácticamente exacta a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, pero que se distribuye de forma totalmente libre, facilitando el acceso a las prestaciones del producto comercial. El Centos Server 7 está basado en RHEL[1] 7 y que entre otras cosas introduce cambios importantes a la virtualización con KVM[2] y que además se ha actualizado para adaptarse al nuevo compilador, gcc 4.4.

4 Fase 4: Implementación de la Honeynet y Pruebas

El host real, con SO Centos Server 7, se conecta directamente al switch paralelo a la red de producción. En este host procedemos a instalar el software de virtualización "VirtualBox" (para más detalle de la instalación véase el Anexo 2**)**, e instalamos las tres máquinas virtuales requeridas en la red Honeynet. La primera máquina virtual es el Honeywall, la segunda es el Honeypot y la tercera maquina utilizada para la administración del Honeywall (Walley), cada una con su respectivo SO anteriormente especificado.

4.1 Configuración de la Red

En la Figura 12, se puede observar el diagrama de la arquitectura y configuración de la Honeynet Virtual, indicando el modo de configuración de cada una de las interfaces de red virtuales y la forma como se interconectan los componentes físicos y virtuales.

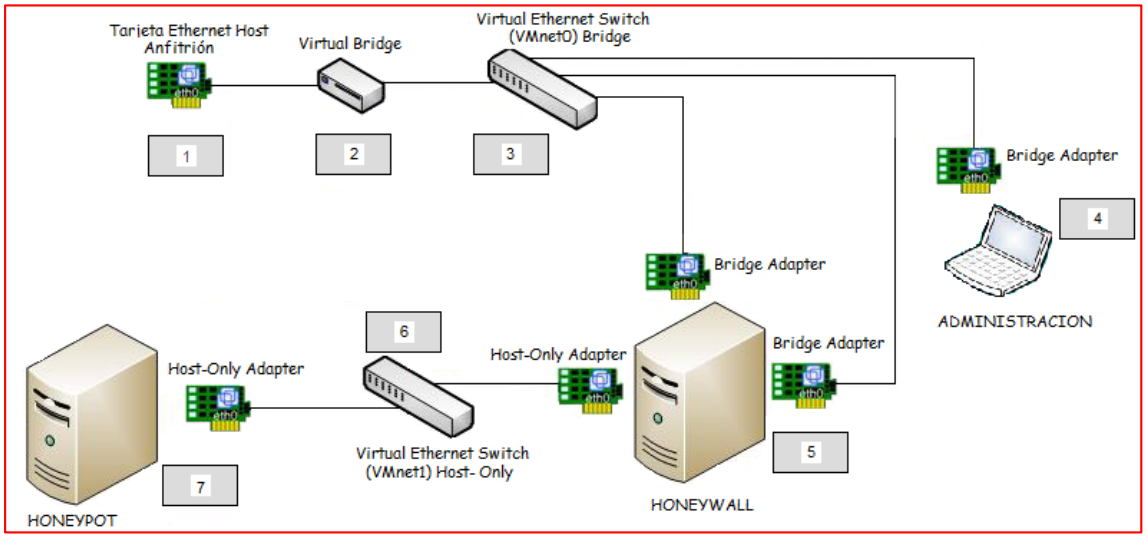


Figura 13: Diagrama Lógico de la Honeynet Virtual

La máquina virtual Honeywall, tiene tres interfaces virtuales de red: (dos en modo bridge y una en modo host-only), el Honeypot posee una interfaz de red en modo hostonly. "El modo host-only permite interconectar máquinas virtuales entre sí, así como también el sistema que las contiene, creando una red privada interna aislada del resto de la red externa. En modo bridge se asocia una interfaz física de red del sistema host por la cual las máquinas virtuales utilizan su propia IP y

les permite acceder y pertenecer al mismo segmento de red a la cual está conectada la máquina que la contiene” [8].

El Honeywall tiene tres interfaces de red la interfaz que está en modo bridge permite la comunicación entre el Honeywall y la red externa, la otra interfaz del Honeywall configurada en modo host-only para comunicase con el Honeypot creando una red entre el Honeywall y el Honeypot independiente y obligando a que el trafico proveniente de la red externa pasen través del Honeywall, si se usara el modo bridge para las interfaces de red de los , estos estarían de igual forma conectados hacia la red externa pero el tráfico no sería registrado ni atravesaría el Honeywall.

4.1.1 Instalación y configuración del Honeywall

Lo primero que se debe hacer es crear la máquina virtual para el Honeywall, es importante cambiar el tipo el disco duro virtual a IDE ya que no será soportado por el sistema que se va a instalar, el cual está basado en Centos.

La máquina virtual se configura con tres tarjetas de red: eth0 y eth2 estén en modo bridge y eth1 en modo host-only. Una guía más detallada sobre la creación y configuración de máquinas virtuales se encuentra en el Anexo 3.

Luego de crear la máquina virtual se procede a la instalación del sistema operativo Honeywall ROO V1.4, que es descargada desde en el sitio web www.honeynet.org. Encendemos la máquina virtual y boteamos la imagen descargada. El proceso de instalación se inicia automáticamente, después de que la instalación esté completa el sistema se reiniciará. Una vez instalado se procede a la configuración. El Honeywall tiene dos cuentas para la administración del sistema por defecto: roo y root, las cuales comparten el mismo password honey.

Para poder ingresar al sistema lo hacemos mediante el usuario roo, y para la configuración necesitamos la cuenta root (con el comando su- podemos pasar a usuario root). Para poder ingresar a la configuración del honeywall se hace uso

del comando /dlg/dialogmenu.sh, este comando nos permite acceder al panel de administración del Honeywall, desde el cual podemos configurar parámetros como: información sobre la red, datos de los Honeypots.

Los principales parámetros a configurar son los siguientes:

TABLA IV: CONFIGURACIÓN DE RED

HONEYPOT	
IP Address	10.1.28.200
Netmask	255.255.252.0
Gateway	10.1.28.1
Broadcast	10.1.31.255
IP Network	10.1.28.0 /22
MANAGER	
IP Address	10.1.28.254
Netmask	255.255.252.0
Gateway	10.1.28.1

Una guía más detallada sobre la instalación y configuración del Honeywall, se encuentra en el Anexo 4.

4.1.2 Instalación y configuración de los Honeypots

Se crean dos máquinas virtuales: una para el Honeypot y la otra para la administración del Honeywall llamada Walleye.

La máquina virtual para el Honeypot deberá tener una tarjeta de red en modo host-only y la máquina virtual para administrador tendrá una tarjeta de red en modo bridge.

Luego de crear las máquinas virtuales cada una con los requerimientos necesarios se procede a instalar el sistema operativo en cada una de estas. Una vez que el sistema operativo ha sido instalado, procedemos a la configuración correspondiente de la interfaz de red.

4.1.3 Configuración de los Servicios

Una vez que tenemos nuestro sistema listo, necesitamos instalar los servicios que la red de producción brinda y estos son: SSH, FTP, HTTP y DHCP.

- DHCP.- (servicio dhcpd) Especifica el rango de direcciones IP, desde la dirección 10.1.28.100/22 hasta la dirección 10.1.28.254/22.

- HTTP.- Se inicia el servicio httpd, ya instalado. La versión del servicio es Apache 2, que ofrece la página web del departamento a los clientes.

- SSH.- Servidor de acceso remoto encriptado. No requiere configuración, basta con iniciar el servicio sshd.

- FTP.- Se instala, configura e inicia el servicio VSFTPD.

Para mayor información y detalle de la instalación de los diferentes servicios, ir al Anexo 5.

4.1.4 Prueba de Funcionamiento correcto de la Honeynet

Una vez que se haya concluido con la instalación y configuración, se realizan pruebas necesarias para con ello garantizar el correcto funcionamiento de la Honeynet, ya que si la red no está funcionando correctamente los datos que se recogerían para hacer el análisis serian incorrectos.

A continuación se listan las pruebas a realizar:

- Los Honeypots deben poder establecer conexiones entrantes y salientes a la red interna usando el protocolo IP:

  Ping entre el Honeypot y el host de administración, ejecutando ping <10.1.28.200>.

  Verificar que se obtiene respuesta con mínimo 4 ECHO replies desde cualquiera de los dos host.

  El Honeypot respondió correctamente, al ping realizado desde el host de administración:

```
root@honeypot:~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@honeypot ~]# ping 10.1.28.254
PING 10.1.28.254 (10.1.28.254) 56(84) bytes of data.
64 bytes from 10.1.28.254: icmp_seq=1 ttl=64 time=1.35 ms
64 bytes from 10.1.28.254: icmp_seq=2 ttl=64 time=0.693 ms
64 bytes from 10.1.28.254: icmp_seq=3 ttl=64 time=0.705 ms
64 bytes from 10.1.28.254: icmp_seq=4 ttl=64 time=0.713 ms
64 bytes from 10.1.28.254: icmp_seq=5 ttl=64 time=0.822 ms
^C
--- 10.1.28.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.693/0.857/1.354/0.253 ms
[root@honeypot ~]#
```

Figura 14: Captura de Pantalla “Ping entre el Honeypot y Host de Administración”

- Los Honeypots deben poder establecer conexiones entrantes y salientes a la red externa usando el protocolo IP:

  Ping desde el host con IP 10.1.30.132 (Host de Prueba), conectado a la red externa, hacia el Honeypot, ejecutando ping <10.1.28.200>.

  Verificar que se obtiene respuesta con mínimo 4 ECHO replies desde cualquier host.

```
[root@roo-test ~]# ping 10.1.28.200
PING 10.1.28.200 (10.1.28.200) 56(84) bytes of data.
64 bytes from 10.1.28.200: icmp_seq=1 ttl=64 time=1.88 ms
64 bytes from 10.1.28.200: icmp_seq=2 ttl=64 time=5.01 ms
64 bytes from 10.1.28.200: icmp_seq=3 ttl=64 time=0.503 ms
64 bytes from 10.1.28.200: icmp_seq=4 ttl=64 time=33.3 ms
64 bytes from 10.1.28.200: icmp_seq=5 ttl=64 time=12.2 ms
64 bytes from 10.1.28.200: icmp_seq=6 ttl=64 time=28.0 ms
64 bytes from 10.1.28.200: icmp_seq=7 ttl=64 time=63.7 ms
64 bytes from 10.1.28.200: icmp_seq=8 ttl=64 time=0.934 ms
64 bytes from 10.1.28.200: icmp_seq=9 ttl=64 time=1.91 ms

--- 10.1.28.200 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8004ms
rtt min/avg/max/mdev = 0.503/16.405/63.793/20.356 ms
[root@roo-test ~]#
```

Figura 15: Captura de Pantalla “Ping entre el Honeypot y Host perteneciente a la red externa”

- Los hosts de la red externa deben poder acceder a los servicios que ofrece el Honeypot. Así podemos comprobar que todos los servicios han sido iniciados y configurados correctamente:

Accedemos desde el host 10.1.30.132 remotamente al Honeypot.

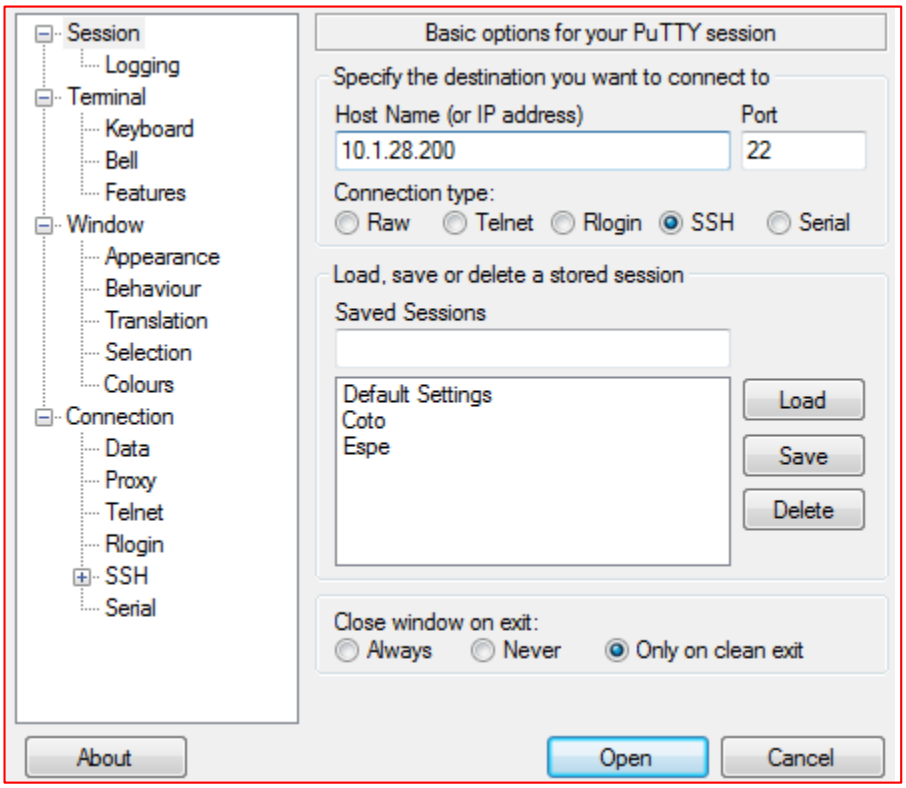


Figura 16: Captura de Pantalla “Sesión SSH utilizando la herramienta Putty”

Accedemos desde el Host de Prueba por medio de un browser, y visualizamos la página web definida en el servidor.

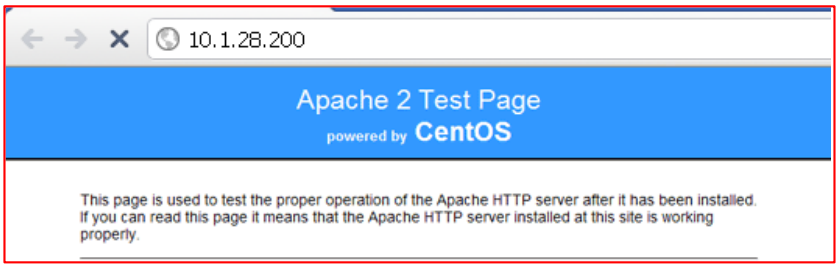
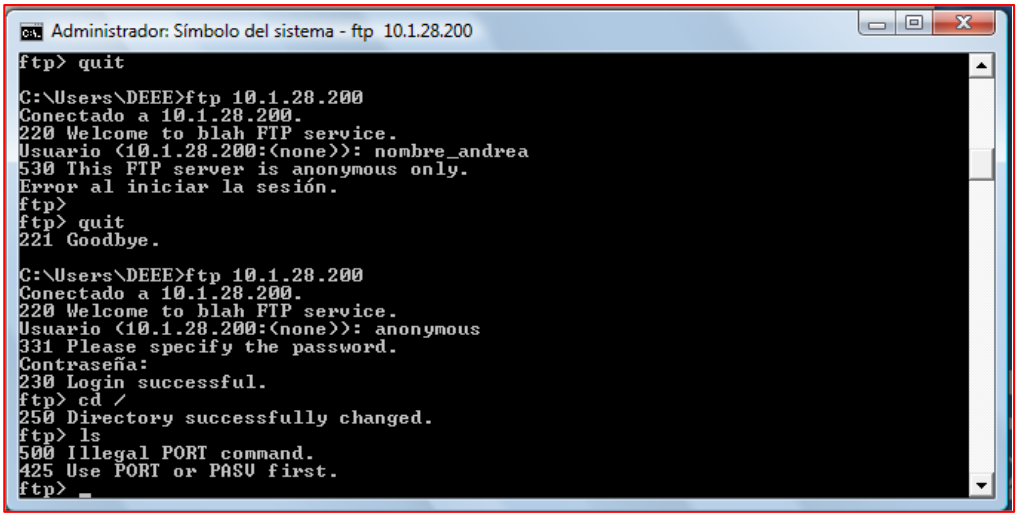


Figura 17: Captura de Pantalla “Página de inicio del Servidor Web”

Desde el host 10.1.30.132, desde línea de comandos, digitamos ftp 10.1.28.200, nos autenticamos por medio del password para proceder a copiar archivos.



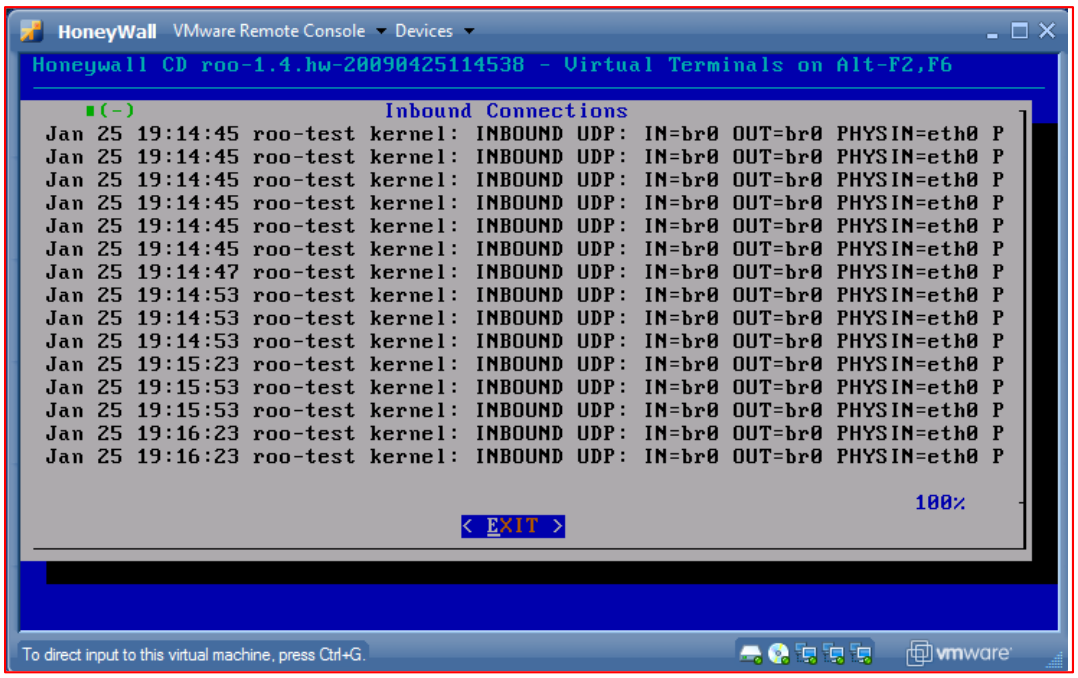
```
ftp> quit

C:\Users\DEEE>ftp 10.1.28.200
Conectado a 10.1.28.200.
220 Welcome to blah FTP service.
Usuario (10.1.28.200:(none)): nombre_andrea
530 This FTP server is anonymous only.
Error al iniciar la sesión.
ftp>
ftp> quit
221 Goodbye.

C:\Users\DEEE>ftp 10.1.28.200
Conectado a 10.1.28.200.
220 Welcome to blah FTP service.
Usuario (10.1.28.200:(none)): anonymous
331 Please specify the password.
Contraseña:
230 Login successful.
ftp> cd /
250 Directory successfully changed.
ftp> ls
500 Illegal PORT command.
425 Use PORT or PASV first.
ftp> _
```

Figura 18: Captura de Pantalla “Servicio FTP desde el Host de Prueba”

El Honeywall está registrando todo el tráfico que circula por la red. Se demuestra observando el incremento en el Inbound y el Outbound.



```
Honeywall CD roo-1.4.hw-20090425114538 - Virtual Terminals on Alt-F2,F6

    (-)                       Inbound Connections
 Jan 25 19:14:45 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:14:45 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:14:45 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:14:45 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:14:45 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:14:45 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:14:47 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:14:53 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:14:53 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:14:53 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:15:23 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:15:53 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:15:53 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:16:23 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P
 Jan 25 19:16:23 roo-test kernel: INBOUND UDP: IN=br0 OUT=br0 PHYSIN=eth0 P

                                                                      100%
                                  < EXIT >
```

Figura 19: Captura de Pantalla “Trafico entrante hacia la Honeynet”

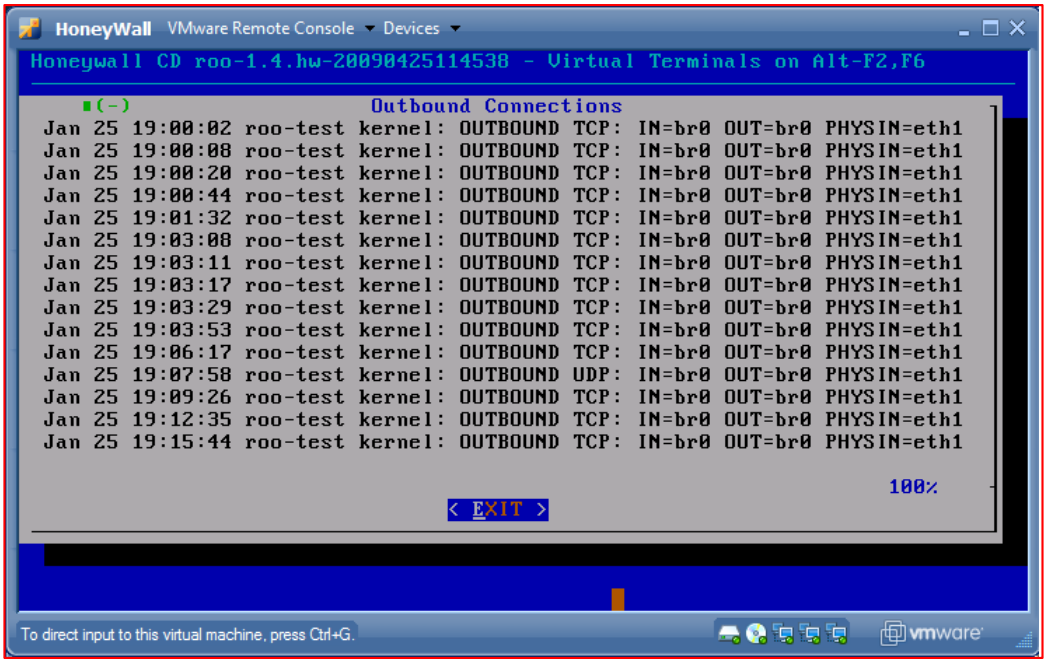


Figura 20: Captura de Pantalla “Trafico saliente desde la Honeynet”

El funcionamiento de Walleye. El host de administración está activado y permite el ingreso. Walleye muestra el tráfico registrado por el Honeywall.

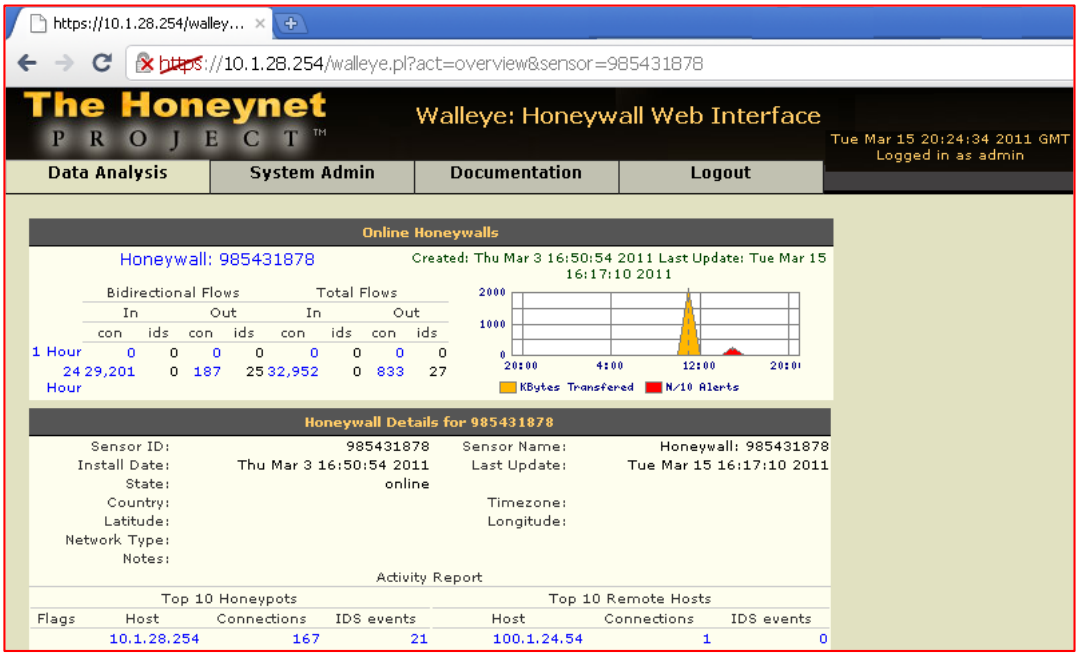


Figura 21: Captura de Pantalla “Interfaz Walleye”

4.1.5 Instalación y configuración de SEC

La instalación de SEC es muy sencilla, lo primero que se debe hacer es descargar el programa, se puede obtener a este paquete en la sección de descargas del sitio web de SEC: http://simple-evcorr.sourceforge.net/.

Los paquetes están disponibles para los sistemas de gestión de paquetes comunes de distribuciones de Linux como Debian, Gentoo, Ubuntu y Fedora. Los pasos para llevar a cabo la instalación son los siguientes:

- Descargar y descomprimir el paquete mediante los siguientes comandos:
  wget http://sourceforge.net/projects/simple-evcorr/files/sec/2.4.beta2/sec-2.4.beta2.tar.gz/download
  tar -zxf sec-2.4.beta2.tar.gz

- Es recomendable copiar los archivos sec.pl (script que es el motor de la correlacion) y sec.man (manual) en las siguientes direcciones:
  cp sec.pl /usr/local/sbin
  cp sec.pl.man /usr/local/man/man8/sec.pl.8

Una vez instalado, solamente hay que crear el script (.conf) y luego ejecutarlo de la siguiente manera: *perl sec.pl -conf=script.conf -input=archivo_patron.*

4.1.6 Configuración del IDS Snort

Para los ataques a desarrollar en el presente proyecto, es necesario realizar ciertas modificaciones en los archivos de configuración del Snort. Se debe descomentar en el archivo /etc/snort/snort.conf las siguientes líneas:

```
#preprocessor arpspoof
# preprocessor frag2
# preprocessor frag3_global: max frags 65536
# preprocessor frag3_engine: policy first detect_anomalies
```

Es necesario además actualizar las reglas para detección de intrusiones. Este procedimiento es fácil de realizar, basta con obtener el código oinkcode, de la página principal de Snort (http://www.snort.org) mediante la creación de una cuenta de usuario que es gratuita y que nos proporciona el oinkcode valido por 30 días y que permite actualizar las reglas de Snort, permitiéndole detectar los

ataques actuales. Para actualizar las reglas en el Honeywall, basta ingresar el oinkcode y las reglas se actualizarán automáticamente.

4.2 Ataques de la Red Honeynet

El objetivo de la implementación de las Honeynets es aprender detalladamente todas las técnicas que utiliza un atacante para llevar a cabo un daño en la red. Por tanto es importante el desarrollo de ataques a los servidores implementados en el Honeypot, como modo de conocer la manera de atacar el servidor, y nos introduce a un ambiente con visión tanto de atacante como de administrador de la red, dándonos una perspectiva más amplia al momento de enfrentar una de estas situaciones.

Pero lo principal, es observar el comportamiento del Honeypot, y como este nos permitirá detectar, analizar y contrarrestar los ataques a los que se ven expuestos los diferentes servicios de nuestra red.

4.2.1 Definición del tipo de Ataque

Se pondrá a prueba la seguridad de la red, y el funcionamiento del Honeywall, llevando a cabo diferentes ataques, del tipo de Denegación de Servicio (DoS), a los diferentes servicios que presta la Honeynet:

- Ataques de Denegación de Servicio

Un ataque de DoS se produce cuando un usuario que posee todos los permisos no puede acceder a un servicio. Tiene como objetivo dar de baja a un host temporalmente (congelándolo), o definitivamente (hasta que se reinicie).

- **Ataque Slowloris:** Se trata de un cliente HTTP capaz de provocar una denegación de servicio (DoS) a servidores web con poco uso de ancho de banda. Entre los servidores web afectados se encuentra tanto Apache 1.x como Apache 2.x.
- **Ataque Hping3:** es un analizador/ensamblador de paquetes TCP/IP de uso en modo consola. Está inspirado en el comando ping de unix, aunque a diferencia de éste, hping no solo es capaz de enviar paquetes ICMP sino que además también puede enviar paquetes TCP, UDP, y RAW-IP.
- **Ataque AMDid:**Conjunto de herramientas para llevar a cabo ataques de DoS y MitM29, dirigidos al servicio de DNS. El único camino por el que el demonio DNS reconoce las diferentes peticiones/respuestas, es la bandera ID del paquete DNS.

Puesto que el DNS genera un ID aleatorio, y a partir de este, solo se incrementa su valor para las siguientes preguntas. Este paquete pretende, realizar el ataque a partir del conocimiento del ID. Entre las herramientas que provee el paquete ADMIDpack están:

- ADMkillDNS - Suplantador de identidad de DNS
- ADMsniffID - Escanea la red, y envía respuestas DNS falsas DNS, antes que el servidor de dominio real.
- ADMsnOOfID - Suplantacion del ID del DNS (requiere ser root en NS)
- ADMnOg00d - Adivina o predice el ID de DNS (no requiere ser root en el NS).
- ADNdnsfuckr – Simple ataque de DoS para deshabilitar el servicio DNS
- ADMkillDNS.- Suplanta la memoria cache del servidor DNS.

4.2.2 Características de los Ataques:

- **Ataque Slowloris:** Un cliente HTTP intenta abrir tantas conexiones como pueda al servidor web e intenta mantenerlas abiertas tanto tiempo como sea posible.

  Periódicamente para evitar que el servidor web cierre la conexión va añadiendo cabeceras a la petición HTTP sin llegar a finalizarla nunca. Provocando así que en los servidores web se vayan quedando las conexiones abiertas hasta llegar al máximo, bloqueando las peticiones legítimas.

  El ataque se lleva a cabo ejecutando el siguiente script:

  # wget http://ha.ckers.org/slowloris/slowloris.pl
  # perl slowloris.pl –dns <IP_VICTIMA_ServidorWeb> □ # perl slowloris.pl –dns 10.1.28.200

- **Ataque ADMdnsfuckr:** Herramienta perteneciente a la suite de ADM. Esta aplicación envía múltiples peticiones PTR 30(resolución inversa IP → dominio) de IPs aleatorias al servidor DNS. Para ello realiza un par de cambios en los paquetes. Por un lado cambia la IP origen (una para cada paquete) empezando siempre en 100.1.10.0 (que es un rango de IPs de las que no se usan). Por otro lado modifica el checksum de la cabecera UDP poniéndolo a 0000, y manda

paquetes erróneos con el fin de que el servidor envié la respuesta correspondiente a cada error.

Para llevar a cabo el ataque, primero se descarga el paquete ADMid-pack, que se puede encontrar en la url http://adm.freelsd.net/ADM/, (descargar el archivo ADMidpkg.tgz). Se procede a descomprimirlo e instalarlo mediante la instrucción make. Hecho esto, basta con ubicarse en el directorio donde se encuentra el archivo ejecutable ADMdnsfuckr (./ADMID-pack/ADMbin/), y ejecutarlo mediante la sentencia:

./ADMdnsfuckr <IP_VICTIMA_ServidorDNS> → # ./ADMdnsfuckr 10.1.28.200

- **Ataque ADMkillDNS:** Para llevar a cabo el ataque basta con ejecutar la siguiente sentencia:

  #./ADMkillDNS<IP_Atacante><IP_Victima_ServidorDNS><Dominio><IP_Dominio>

- **Ataque Hping3:** Para llevar a cabo este ataque, basta con hacer uso del siguiente comando:

  #hping3 –S –p 80 <IP_Victima_ServidorWEB>

4.2.3 Software involucrado para las intrusiones

Para poder determinar estos dos tipos de ataques se necesita varios módulos que requieren ser instalados. A continuación se detallan cada uno de ellos:

- **Ataque Slowloris:** Para usar slowloris necesitaremos los siguientes módulos de perl:

  perl –MCPAN –e 'install GetOpt::Long'

  perl –MCPAN -e 'install IO::Socket::INET'

  perl –MCPAN -e 'install IO::Socket::SSL'

- **Ataque ADMid:** Para usar las herramientas de ADMid se requiere instalar los siguientes paquetes:

  ADMID-pack

g. Discusión

El presente trabajo de titulación, expone a la comunidad universitaria las ventajas de tener una Honeynet como mecanismo de seguridad informática, siendo como objetivo principal de la misma reunir información sobre la actividad del intruso. Logrando así detectar las vulnerabilidades que posee la red antes de que estas sean explotadas. Una de las ventajas de las Honeynets es que nos proveen de la inteligencia necesaria para conocer los riesgos con los que se cuenta en la red de datos de la Universidad Nacional de Loja.

1. Desarrollo de la Propuesta Alternativa

Objetivo 1: Describir la situación actual de la infraestructura de la red de datos de la UNL, para determinar sus puntos críticos.

Para su cumplimiento se llevó a cabo mediante observación directa a la red de datos de la Universidad Nacional de Loja (Sección 1.1 de la Fase 1), en la cual se determinaron sus características, entre ellas tenemos: ancho de banda y proveedor de internet (CEDIA).

Un análisis sistemático del centro de cómputo, tomando en cuenta el equipo hardware, el nivel de seguridad tanto física como lógica y las políticas que se aplican actualmente en el Departamento de Telecomunicaciones (Sección 1.2 de la Fase 1), permitieron definir las buenas prácticas para contrarrestar los puntos críticos de la red de datos de la Universidad Nacional de Loja.

Objetivo 2: Analizar y seleccionar el tipo de Honeynet conjuntamente con los equipos necesarios para su posterior implementación.

El presente objetivo se lo cumplió, realizando una síntesis bibliográfica de los casos de éxito de implementación de Honeynets en instituciones de educación superior, tomando en cuenta como aspecto principal la arquitectura de una Honeynet (Sección 2.1 de la fase 2), posteriormente se hace la selección del mejor tipo de Honeynet (Sección 2.2 de la Fase 2), en base a los requerimientos, objetivos, equipo hardware disponible en el centro de cómputo del Departamento de Telecomunicaciones e Información y recursos humanos (indirectos) que de una u otra manera actuaron en el proceso de desarrollo del presente proyecto

Se determinó la técnica de implementación de la Honeynet, sin dejar de lado la realidad de la universidad (Sección 2.3 de la Fase 2). Se determinó la estructura de la Honeynet en cuanto al tipo, las herramientas necesarias y la técnica más eficiente de implementación (Sección 2.4 de la Fase 2).

En esta fase se ha determinado una base firme para el diseño e implementación de una Honeynet Virtual de Generación III Autocontenida, la cual da la ventaja de estar un paso adelante del enemigo, permitiendo así aprender cuanto sea posible de las amenazas y del comportamiento de los atacantes, para implantar una arquitectura de seguridad proactiva que permita no sólo defendernos de tales amenazas, si no también someterlas antes de que sucedan

Objetivo 3: Diseñar el diagrama de la red de datos con la topología de la Honeynet.

El presente objetivo se cumplió realizando un diseño de la Honeynet dentro de la red de datos de la Universidad Nacional de Loja (Sección 3.1 de la Fase 3), detallando cada una de las principales características que tiene la Honeynet. Así se detalla el equipo físico que contiene a las máquinas virtuales (Honeypot y Honeywall) para su posterior implementación.

Se determina el Software de virtualización que tendrá el host anfitrión, para poder levantar las máquinas virtuales q son los elementos de la Honeynet (Sección 3.2 de la Fase 3), posteriormente se determinan cada uno de los sistemas operativos que tienen los diferentes elementos de la Honeynet (Sección 3.3 de la Fase 3), cabe recalcar que el Honeywall CDROM incorpora sólo las herramientas necesarias para que ese sistema funcione (Sección 3.4 de la Fase 3).

Objetivo 4: Implementar y configurar las herramientas de la Honeynet en escenarios de pruebas reales para su evaluación.

El presente objetivo se lo dividió en varias partes para cumplirlo en su totalidad. Primero se realizó la configuración de la red con los diferentes equipos que conforman la Honeynet (Secciones 4.1.1 – 4.1.2 de la Fase 4), se procede a levantar los diferentes servicios que están configurados en el Honeypot (Sección 4.1.3 de la Fase 4). Después de realizar todas las configuraciones se realizan las diferentes pruebas para verificar el funcionamiento correcto de la Honeynet (Sección 4.1.4 de la Fase 4). Posteriormente se realiza la instalación de dos herramientas (SEC, IDS Snort) que van a controlar los diferentes ataques a los cuales se somete la red.

2. Valoración Técnica Económica Ambiental

El desarrollo del presente trabajo de titulación, exigió una inversión económica, la que permitió lograr el resultado final, que fue alcanzar los objetivos planteados, evidenciándose en cada una de las fases especificadas en los resultados del mismo, a continuación se detalla la inversión económica:

TABLA V: PRESUPUESTO

PRESUPUESTO				
RECURSOS HUMANOS				
Descripción	Cantidad	Núm. de Horas	Valor Unitario	Valor Total
Carlos Heredia	1	936	10	9360,00
Director de Tesis	1	100	0	0,00
			SUBTOTAL	9360,00
RECURSOS MATERIALES				
MATERIALES DE OFICINA				
Papel (Resma)	3	—	3,50	10,50
Cartuchos	4	—	5,00	20,00
Fotocopias	500	—	0,02	10,00
Anillados	3	—	2,00	6,00
CD's	3	—	1,00	3,00
			SUBTOTAL	49,50
SERVICIOS BÁSICOS				
Transporte	----	—	0,25	100,00
Comunicación	36	—	1,00	36,00
Internet	----	---	0.00	00,00
			SUBTOTAL	136,00
RECURSOS TÉCNICOS TECNOLÓGICOS				
HARDWARE				
Portátil HP G42	1	936	800,00	800,00
Flash Memory	1	—	10,00	10,00

Impresora	1	—	180,00	180,00
			SUBTOTAL:	990,00
SOFTWARE				
Centos 7.0	1	936	0,00	0 , 00
Servidor UNL	1	—	0,00	0 , 00
Honeywall CDROM	1	936	0,00	0 , 00
Virtual Box	1	936	0,00	0 , 00
Libre Office	1	936	0,00	0 , 00
			SUBTOTAL	0 , 00
			TOTAL	**10.535,50**

El presente proyecto se desarrolló, utilizando herramientas con licencia libre, reduciendo notablemente el costo de recursos materiales, en su totalidad el costo fue asumido por el autor del proyecto de titulación, excepto el costo del recurso humano del director, ya que ese valor es adjudicado por la universidad.

h. Conclusiones

Después de haber realizado el presente proyecto fin de carrera se concluye lo siguiente:

- La importancia del análisis de la red en el desarrollo del proyecto permitió determinar puntos críticos, servicios vulnerables, las intrusiones a las que está más propensas a realizarse, los puertos que están habilitados, el porcentaje de tráfico que circula por esta, etc. Esta información fue de gran utilidad ya que ayudó a generar las reglas de detección y analizar el tráfico en la red al momento de generar un ataque
- La Honeynet por virtualización entrega una solución rentable económicamente, ya que permite movilidad y ahorro de espacio y hardware, además de un alto rendimiento, utilizando un software de virtualización estable.
- La Honeynet utiliza de manera estándar un correlacionador de eventos llamado Sebek, en este proyecto se optó por utilizar una nueva herramienta llamada SEC que se programa en lenguaje perl para realizar la correlación de eventos. SEC permite obtener resultados satisfactorios ya que detectó ataques ignorados por el IDS además de desechar falsos positivos, detectados por el IDS.
- Las pruebas realizadas y el análisis de los resultados obtenidos nos permite concluir que el sistema ha funcionado correctamente y ha logrado detectar los diferentes ataques que se ha llevado acabo, generando las respectivas alertas; logrando así tener un monitoreo de todo el tráfico que circulan en la red, y cumpliendo con los objetivos establecidos.
- Mediante la implementación de la Honeynet se logró determinar las vulnerabilidades y puntos críticos de la red, para recolectar toda la información acerca del atacante y su modo de operación. Permitiendo de esta manera estar un paso adelante que el enemigo y mantener la red de datos protegida.

i. Recomendaciones

Al terminar el proyecto fin de carrera se puede recomendar lo siguiente:

- Ubicar la Honeynet en un segmento de red libre de elementos que modifiquen los paquetes que circulan en la red; como por ejemplo, no ubicarla detrás de un firewall que haga NAT o traducción de direcciones, para que así el Honeywall pueda detectar las direcciones IP que realizan peticiones a la red, sin que se produzca enmascaramiento.
- Se recomienda prestar atención al implementar una Honeynet debido a la complicidad, protección de datos y responsabilidades por cualquier daño que es capaz de causarse desde el Honeypot. Por tanto es importante un monitoreo constante de la red y ubicar la Honeynet en una zona donde no comprometa a ningún sistema y evitar que alguna red sufra daños.
- Para que la Honeynet tenga un mejor rendimiento, se recomienda hacer uso de la gran variedad de herramientas que se pueden instalar y emplear en el Honeywall. Para mantener la estabilidad y seguridad de la Honeynet entre las herramientas se recomienda utilizar se incluyen POF (Passive OS Fingerprint) que analiza el tráfico de la red e intenta identificar el sistema operativo en base a parámetros TCP/IP, SWATCH (Simple Watcher Off Logfiles) que investiga los archivos de logs del Honeywall en busca de eventos definidos mediante expresiones regulares y envía un correo al administrador si encuentra alguna actividad de red sospechosa.

j. Bibliografía

[1] ALEGSA. Diccionario de Informática. En línea, link [http://www.alegsa.com.ar/Dic/honeypot.php], consulta [11-11-2013].

[2] Introducción a las Honeynets. Universidad Autónoma de México. En línea, link [http://www.asc.unam.mx/descarga.dsc?arch=247], consulta [11-11-2013].

[3] M. Dornseif, F.C. Gartner, and T. Holz. Vulnerability Assessmentusing Honepots. En línea, link [http://www.ei.rub.de/media/emma/veroeffentlichungen/2013/03/03/vulnerability-assessment-using-honepots.pdf.], consulta [11-11-2013].

[4] HoneyNets, una desconocida en la seguridad informática. En línea, link [http://www2.fe.ccoo.es/andalucia/docu/p5sd6337.pdf.], consulta [11-11-2013].

[5] Pedro P. HONEYPOTS Y HONEYNETS. Academia Madesyp. En línea, link [http://www.slideshare.net/navajanegra_ab/charla-honeypots], consulta [11-11-2013].

[6] Gabriel García. Introducción a los Honeypots. Revista: Linux Noviembre 2007 (N°37). En línea, link [http://www.the-evangelist.info/2011/09/ introduccion-a-los-honeypots/], consulta [11-11-2013].

[7] Niels Provos; Thorsten Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison Wesley professional, 2007.

[8] Jorge Isaac Avilés Monroy, Mayra Rosibel Pazmi˜no Castro. Captura y Análisis de los Ataques Informáticos que sufren las Redes de Datos de la ESPOL, implantando una Honeynet con miras a mejoar la Seguridad Informática en Redes de Datos del Ecuador. Escuela Superior Politécnica del Litoral. Tesis de grado. En línea, link [www. cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-39239.pdf], consulta [20-11-2013].

[9] The Honeynet Project. Know Your Enemy: Honeynets. 2006. En línea, link [http://honeynet.org/papers/honeynet/], consulta [20-11-2013].

[10] Eduardo Gallego, Jorge López de Vergara. Honeynets: Aprendiendo del Atacante. Universidad Politécnica de Madrid. En línea, link [https://web.dit.upm.es/˜jlopez/publicaciones/mundointernet04.pdf], consulta [20-11-2013].

[11] Jorge Aviles Monro, Mayra Pazmiño Castro. Captura y análisis de los ataques informáticos que sufren las redes de datos de la ESPOL, implantando una Honeynet con miras a mejorar la seguridad informática en redes de datos del Ecuador.

Escuela Superior Politécnica Del Litoral. En línea, link [www.dspace.espol.edu.ec/handle/ 123456789/4203?mode=full], consulta [20-11-2012].

[12] Fingerprinting. En línea, link [http://nmap.org/nmap-fingerprinting-article-mx.html], consulta [21-11-2013].

[13] Alberto Segovia. Honeynets IV: Tareas y Herramientas. Security Artwork. 06-06-2010. En línea, link [http://www.securityartwork.es/2010/07/06/ honeynets-iv-tareas-y-herramientas/], consulta [20-11-2013].

[14] Sistemas de Detección de Intrusos y Snort. Maestros del Web. Publicado en Agosto 19, 2013. En línea, link [http://www.maestrosdelweb.com/editorial/snort/], consulta [20-11-2013].

[15] Tu Quiosco de Conocimientos. Productos virtualización: VMWare. En línea, link [http://tuquiosco.es/virtualizacion/productos-virtualizacion-vmware/], consulta [20-11-2013].

[16] TELCONET. Servicios que ofrecemos. En línea, link [http://telconet.bumeran.com.ec/telconet.bum], consulta [22-05-2014].

[17] CEDIA. Quienes Somos. En línea, link [http://www.cedia.org.ec/index.php/cedia11/quienes-somos], consulta [22-05-2014].

[18] CEDIA. Red Avanzada. CEDIA. En linea, link [http://www.cedia.org.ec/index.php/red-avanzada], consulta [28-05-2014].

[19] Dr. Enrique Peláez. Desarrollo de LA RED ACADÉMICA ECUATORIANA – Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado. CEDIA. Consulta [28-05-2014].

[20] M.Sc.Ing. Hernán Leonardo Torres Carrión. Administración de Centros de Cómputo. Unidad de Octavo Módulo. Universidad Nacional de Loja. Consulta [26-05-2014].

[21] Material emitido por el Departamento de Telecomunicaciones e Información (UTI). Departamento de Redes. Universidad Nacional de Loja. Consulta [01-04-2014].

[22] Cristian F. Borghello. (2001). Tesis: Seguridad Informática, sus Implicancias e Implementación. En línea, linkl [http://www.segu-info.com.ar/tesis/], consulta realizada [02-07-2014].

[23] Gabriel Marcos. (2011). Redundancia, Contingencia, Continuidad, Resiliencia. Recuperado el [02-07-2014] de la página web CompuChannel.net. En línea, link [http://www.compuchannel.net/2011/04/03/redundancia-contingencia-continuidad-resiliencia/].

[24] Firewalls de última generación Cisco ASA serie 5500. CISCO. En línea, link [http://www.cisco.com/web/ES/products/security/asa_5500_series_next_ generation_firewalls.html], consulta [28-05-2014].

[25] Introducción a las Honeynets. Universidad Autónoma de México. En línea, link [http://www.asc.unam.mx/descarga.dsc?arch=247], consulta [11-11-2013].

[26] Jorge Isaac Avilés Monroy, Mayra Rosibel Pazmiño Castro. Captura y Análisis de los Ataques Informáticos que sufren las Redes de Datos de la ESPOL, implantando una Honeynet con miras a mejorar la Seguridad Informática en Redes de Datos del Ecuador. Escuela Superior Politécnica del Litoral. Tesis de grado. En línea, link [www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-39239.pdf], consulta [20-11-2013].

[27] Pedro P. HONEYPOTS Y HONEYNETS. Academia Madesyp. En línea, link [http://www.slideshare.net/navajanegra_ab/charla-honeypots], consulta [11- 11-2013].

[28] Gabriel García. Introducción a los Honeypots. Revista: Linux Noviembre 2007 (No 37). En línea, link [http://www.the-evangelist.info/2011/09/ introduccion-a-los-honeypots/], consulta [11-11-2013].

[29] The Honeynet Project. Know Your Enemy: Honeynets. 2006. En línea, link [http://honeynet.org/papers/honeynet/], consulta [20-11-2013].

[30] Eduardo Gallego, Jorge López de Vergara. Honeynets: Aprendiendo del Atacante. Universidad Politécnica de Madrid. En línea, link [https://web.dit.upm.es/~jlopez/publicaciones/mundointernet04.pdf], consulta [20-11-2013].

[31] Tú Quiosco de Conocimientos. Productos virtualización: VMWare. En línea, link [http://tuquiosco.es/virtualizacion/productos-virtualizacion-vmware/], consulta [20-11-2013].

[32] M. Dornseif, F.C. G¨artner, and T. Holz. Vulnerability Assessmentusing Honepots. En línea, link [http://www.ei.rub.de/media/emma/veroeffentlichungen/2013/03/03/vulnerability-assessment-using-honepots.pdf.], consulta [11-11-2013].

[33] HoneyNets, una desconocida en la seguridad informática. En línea, link [http://www2.fe.ccoo.es/andalucia/docu/p5sd6337.pdf.], consulta [11-11-2013].

[34] HoneyNets, una desconocida en la seguridad informática. En línea, link [http://www2.fe.ccoo.es/andalucia/docu/p5sd6337.pdf.], consulta [11-11-2013].

[35] Niels Provos; Thorsten Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison Wesley professional, 2007.

[36] Fingerprinting. En línea, link [http://nmap.org/nmap-fingerprinting-article-mx.html], consulta [21-11-2013].

[37] Alberto Segovia. Honeynets IV: Tareas y Herramientas. Security Artwork. 06-06-2010. En línea, link [http://www.securityartwork.es/2010/07/06/honeynets-iv-tareas-y-erramientas/], consulta [20-11-2013].

[38] Sistemas de Detección de Intrusos y Snort. Maestros del Web. Publicado en Agosto 19, 2013. En línea, link [http://www.maestrosdelweb.com/editorial/snort/], consulta [20-11-2013].

k. Anexos

Anexo 1: Contrato de Internet de la Universidad Nacional de Loja.

UNIVERSIDAD NACIONAL DE LOJA

UNIDAD DE CONTRATACIÓN PÚBLICA

IN THE SAVRIS SAPIENTIAE

d) **"LOSNCP"**, Ley Orgánica del Sistema Nacional de Contratación Pública.

e) "**Oferente**", es la persona natural o jurídica, asociación o consorcio que presenta una "oferta", en atención al llamado a Menor Cuantía;

*f) "**Oferta**", es la propuesta para contratar, ceñida a los pliegos, presentada por el oferente a través de la cual se obliga, en caso de ser adjudicada, a suscribir el contrato y a la ejecución de la* CONTRATACIÓN DEL SERVICIO DE INTERNET Y RED AVANZADA PARA LA UNIVERSIDAD NACIONAL DE LOJA

Cláusula Cuarta.- OBJETO DEL CONTRATO

4.01.- El contratista se obliga con la CONTRATANTE a cumplir con la CONTRATACIÓN DEL SERVICIO DE INTERNET Y RED AVANZADA PARA LA UNIVERSIDAD NACIONAL DE LOJA a entera satisfacción de a CONTRATANTE, de conformidad con los requerimientos institucionales.

Ítem	*Descripción*
CONDICIONES GENERALES	▪ El proveedor debe de incluir en el Contrato de Prestación del Servicio una Red Avanzada de Distribución Nacional con conexión Internacional, y que adicionalmente tenga el servicio de Internet Comercial con una distribución de últimas millas red nacional y enlaces internacionales según las condiciones descritas en el presente documento.
	▪ Esta **red de distribución nacional** debe ser basada en una infraestructura de fibra óptica que conecte a todos los miembros de Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado – CEDIA. Esta red nacional debe estar conectada al nodo de red Avanzada en Guayaquil que da enlace internacional con Red Consorcio Latinoamericano de Redes Avanzadas – CLARA y a todas las redes avanzadas del mundo.
CONDICIONES TÉCNICAS	A continuación, se definen los criterios técnicos para los enlaces de última milla, enrutamiento, interfaces, y administración de la red. Las últimas millas deben ser de fibra óptica de acuerdo a las condiciones que se describen:
	▪ El ancho de Banda para Internet Comercial que se requiere será de 99,00 Mbps, a partir de la firma del contrato.
	▪ Los medios tecnológicos de última milla serán punto a punto, no compartido, con interfaces mínimas Gigabit Ethernet, y capacidad de procesamiento de 1Gbps real. Los tiempos máximos de retardos permitidos serán de 15 milisegundos hasta el nodo de salida internacional definido por el

	proveedor, sin pérdida de paquetes. De manera general la últimas millas debe garantizar baja sensibilidad al jitter, cambio de cadencia en el tren de información, y libres c congestión, todo esto podrá ser monitoreado por la institución
	▪ Enlace tipo IP (full duplex) hasta la interfaz d comunicaciones de la institución.
	▪ El protocolo de enrutamiento a implementarse será BGP (con soporte MPBGP).
	▪ Visualización de la configuración de los equipos, y del servicio de Internet, incluido protocolos de administración de redes (SNMP, RMON) con el objetivo de monitorear las configuraciones del servicio de Internet propio
	▪ Capacidad de servicio de VPN para la comunicación entre l diferentes campus, a través de MPLS, garantizando un MTU de 1500 bytes así como también jumbo frames.
ENLACE AL NAP NACIONAL e INTERNACIONAL	▪ El ancho de banda contratado no debe ser compartido (Clear Channel), y debe cumplir con las capacidades y condiciones establecidas en el presente documento. De manera general se garantiza baja sensibilidad al jitter o cambio de cadencia en el tren de información, y una conexión libre de congestión con latencias promedio permitidas de 110 ms desde el CPE de la Institución hasta sitios web en EEUU como Yahoo o Google
	▪ La capacidad de Internet será provista a través de una conexión directa con varios proveedores TIER 1 para redundancia
ENLACE A CLARA	▪ Conexión del nodo de CEDIA-Guayaquil con el POP CLAR de Guayaquil a través de un enlace Gigabit Ethernet, con un tiempo de retardo no mayor a 30ms, desde los CPE de la Institución al ruteador del POP CLARA en Guayaquil
	▪ Acceso de lectura/escritura y protocolos de administración del equipo a instalarse en el proveedor para conexión con el POP CLARA Guayaquil (último ruteador del proveedor del servicio que se comunica al POP de CLARA). Deben estar disponibles los protocolos de administración de redes (SNMP, RMON) con el objetivo de monitorear las configuraciones del servicio.
	▪ Acceso compartido al Ancho de Banda de mínimo 45Mbps para conexión a la Red CLARA contratado por el proveedor.
ENLACE ENTRE MIEMBROS DE CEDIA	▪ Conexión con el NAP Ecuador con un tiempo máximo de retardos de 40ms, desde el CPE de la Institución a los ruteadores del POP de Aeprovi en Quito y Guayaquil.

Anexo 2: Instalación y Configuración de Virtual Box.

Instalación de Paquetes Requeridos

Antes de instalar VirtualBox, es necesario instalar algunos prerrequisitos:

- Librerías de Desarrollo (Development Libraries)
- Herramientas de Desarrollo (Development Tools)
- Paquete xinetd
- Paquete kernel-devel.

Instalación de VirtualBox

1. Descargar
2. Descomprimir el archivo

Configuración de VirtualBox

Esta es la interfaz del programa una vez que se encuentra instalado correctamente.

Figura 22: Interfaz de VirtualBox.

Una vez que se encuentra instalado el programa no se requieren realizar configuraciones, ya que éstas serán realizadas en el proceso de creación de cada una de las máquinas virtuales.

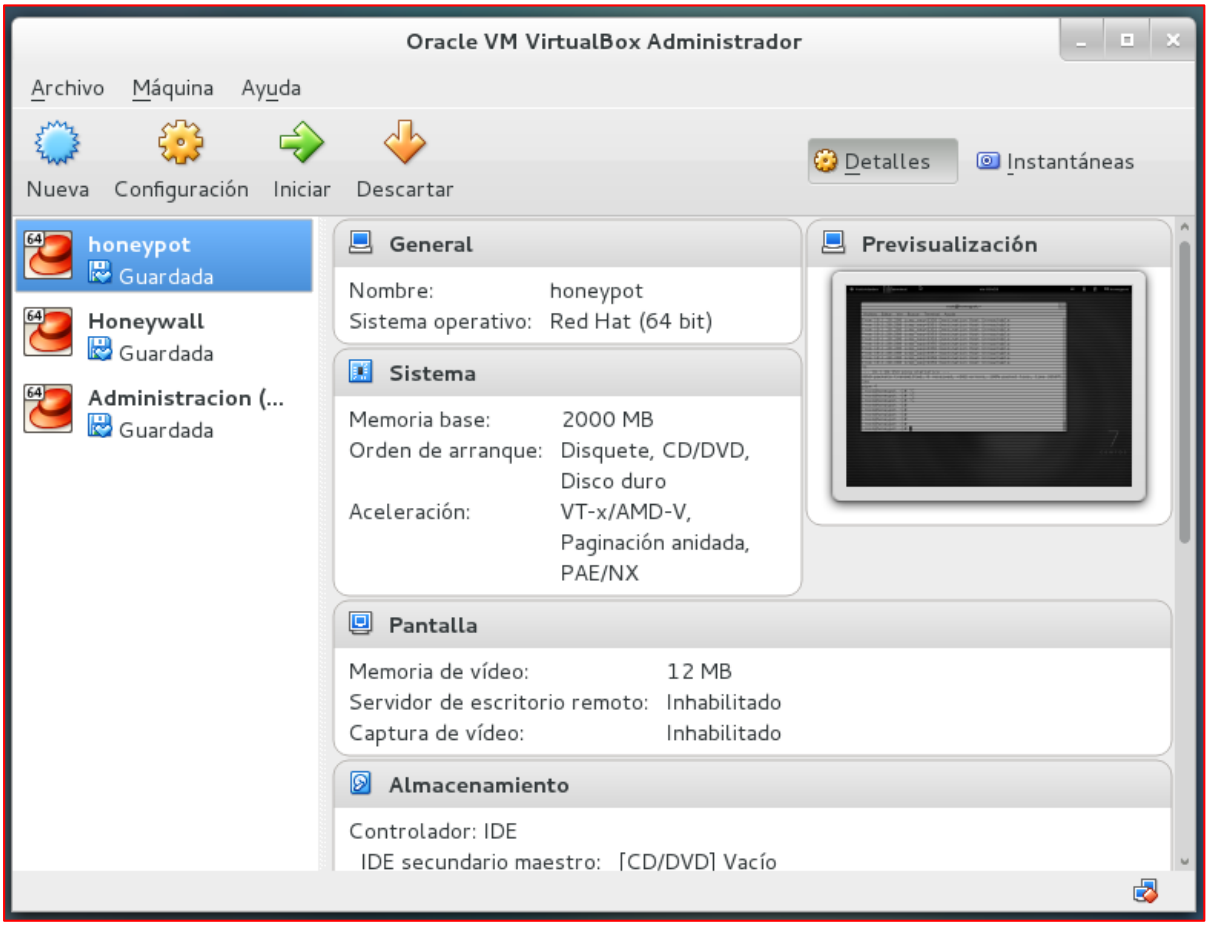


Figura 23: Creación de las máquinas Virtuales.

Anexo 3: Configuración de las Máquinas Virtuales.

Una vez que ya se encuentra el virtualizador instalado se procede a realizar la creación y levantamiento de las máquinas virtuales necesarias para la implementación de la Honeynet.

Se realizan los siguientes procesos para crear una máquina virtual:

Se debe dar click en el botón de nueva máquina virtual y se coloca el nombre con el cual se va a definir la máquina virtual creada.

Figura 24: Nombre de la Máquina Virtual

Se asigna una cantidad de memoria RAM que va a tener la máquina virtual, esto depende de las funciones que vaya a desempeñar la misma.

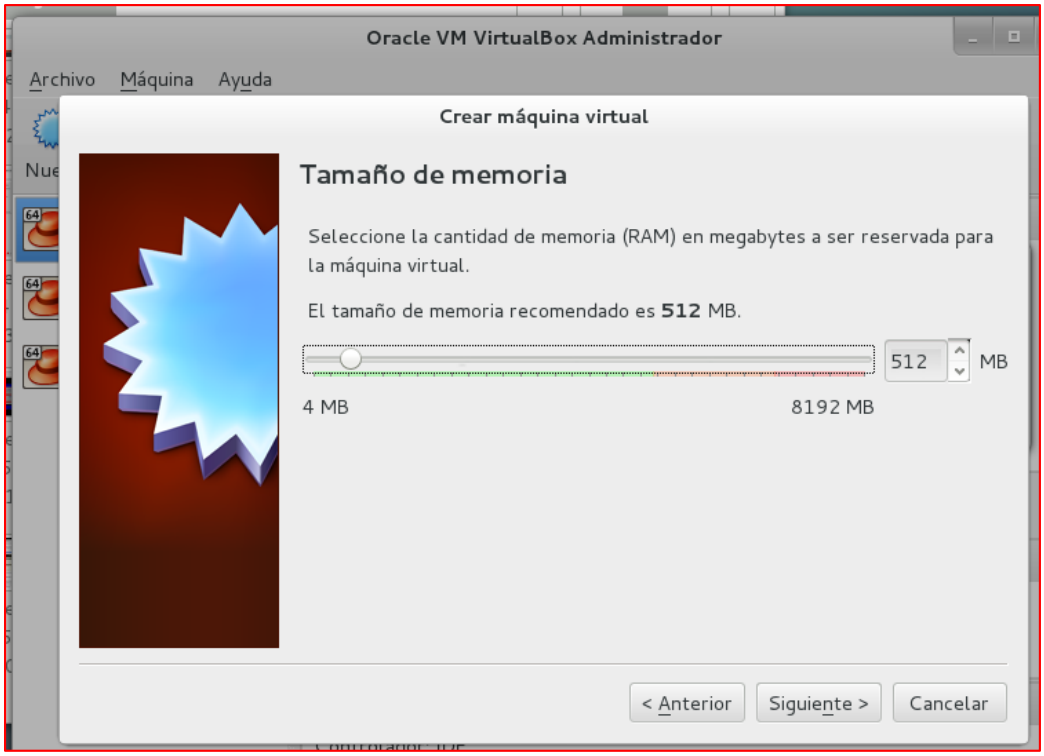


Figura 25: Tamaño de Memoria

Se asigna la cantidad de disco duro que va a tener la máquina virtual, depende de la capacidad total del disco duro físico de la computadora que va a contener a las máquinas virtuales.

Figura 26: Unidad de disco Duro.

Seleccionar el tipo que va a tener el disco duro de la máquina virtual, se recomienda dejarlo por defecto la opción marcada automáticamente por el VirtualBox.

Figura 27: Tipo de Archivo de Unidad de Disco Duro.

Anexo 4: Instalación y Configuración del Honeywall ROO v1.4.

Pasos para la instalación del Honeywall.

Presionar el botón Enter, para que el sistema comience a sobre escribir la unidad de disco duro existente y así comenzar el proceso de instalación.

Figura 28: Inicio de la instalación del Honeywall

Después de que la instalación se ha completado con éxito, el sistema se reiniciará automáticamente, presentando una consola de comando, donde podrá iniciar sesión y comenzar el proceso de configuración del Honeywall.

Acceso al Sistema

Para ingresar a la administración como usuario root, obligadamente se debe iniciar antes como usuario roo, la contraseña para estos usuarios es honey por defecto.

Configuración de las Variables.

Iniciar la configuración ingresando al directorio dlg y ejecutando la aplicación ./dialogmenu.sh

Figura 29: Pantalla de advertencia del Honeywall.

Para proceder a configurar el Honeywall se debe Seleccionar Honeywall Configuration.

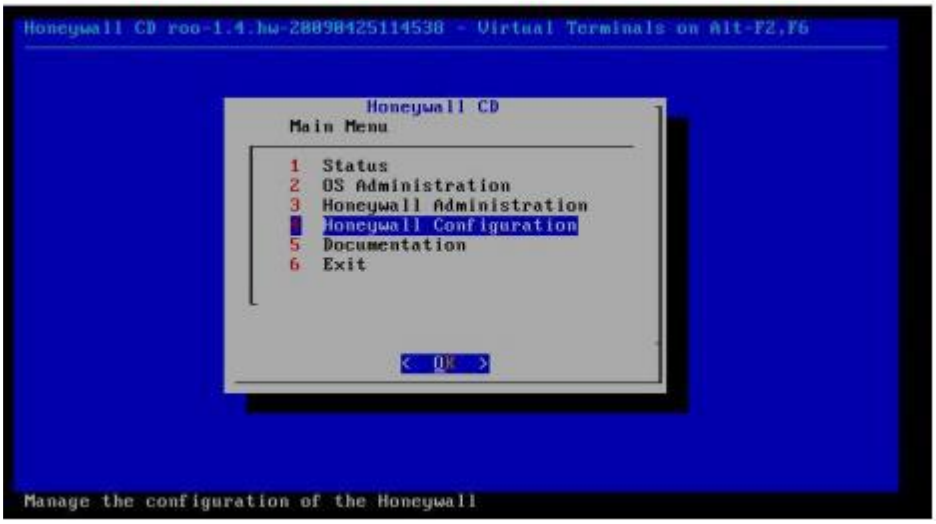


Figura 30: Inicio de la Configuración del Honeywall.

El tipo de configuración que se realizara pueden ser estas dos opciones:

a) FLOPPY: El honeywall permite cargar configuraciones existentes almacenadas en un disquete.
b) INTERVIEW: Elegir si se va a configurar por primera vez.

Figura 31: Selección del tipo de Configuración.

Ingrese las direcciones IPs de todos los honeypots separados por un espacio.

Figura 32: Ingreso de las Direcciones Ips de los Honeypots.

Ingrese las direcciones IP de la Honeynet.

Figura 33: Ingreso de la dirección IP de la Honeynet.

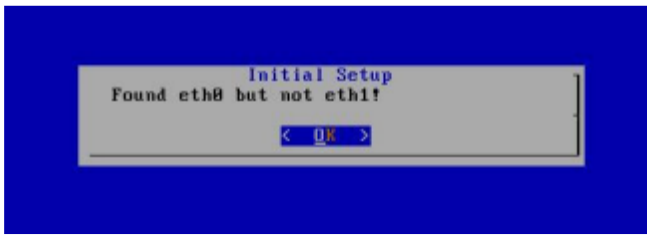


Figura 34: Interface eth0 y eth1 encontrada.

Ingrese la dirección de broadcast correspondiente a la red de la Honeynet.

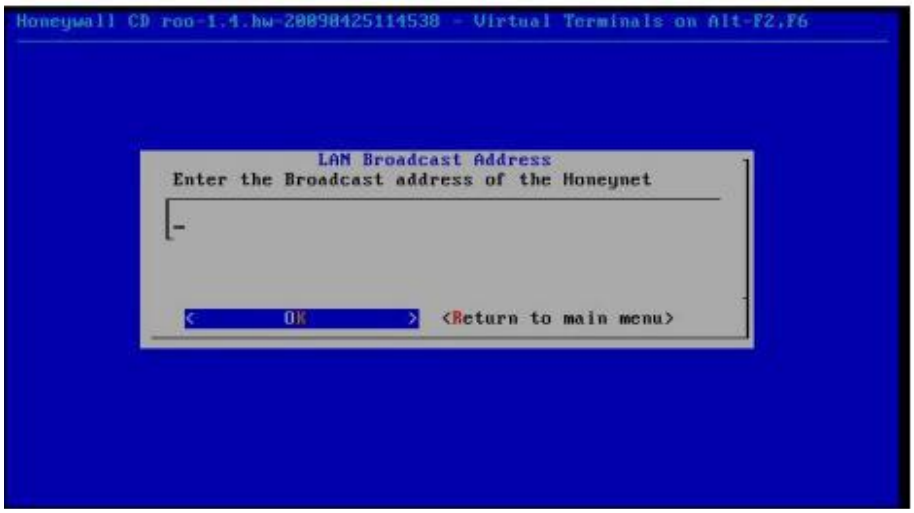


Figura 35: Ingreso de las direcciones broadcast de la red LAN.

Posteriormente se procede a la configuración de la interfaz remota de administración.

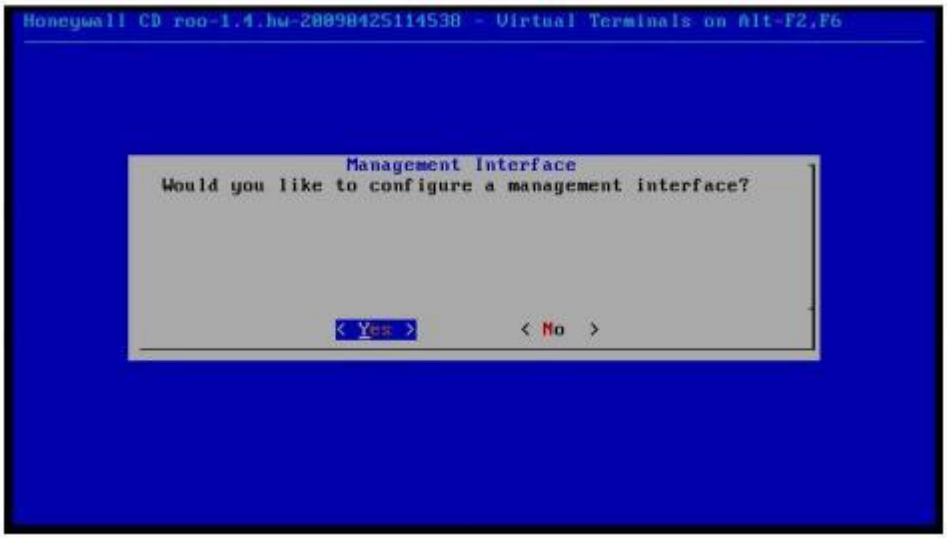


Figura 36: Inicio de la configuración de interface de administración.

Configuración SSH

Figura 37: Inicio de la Configuración de SSH

Permitir el logearse por SSHD

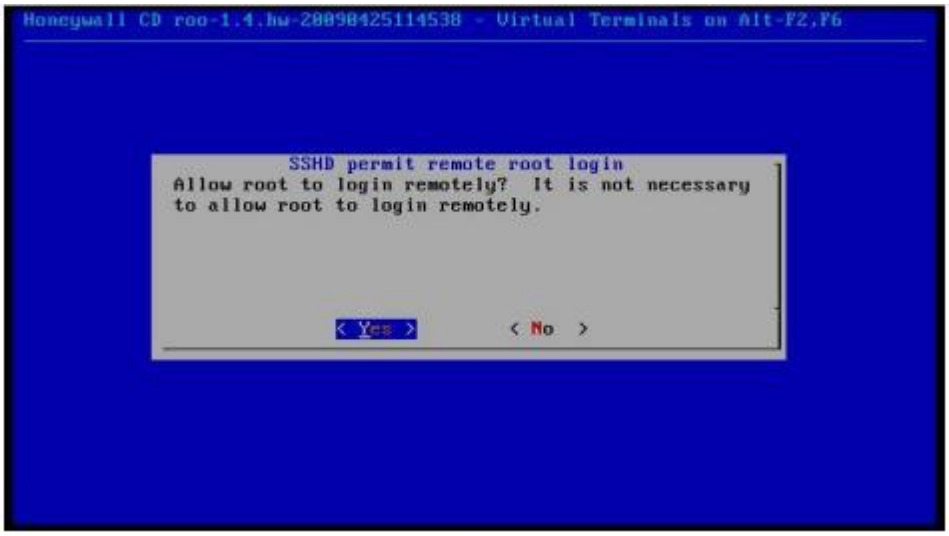


Figura 38: Login remotamente como root

Cambiar el password de los usuarios que traen por defecto el sistema Honeywall, elegir la contraseña más segura por el administrador.

Figura 39: Cambio de contraseña de root.

Figura 40: Cambio de contraseña de roo

Ingresar una lista de puertos TCP permitidos para la interfaz de administración, por defecto está incluido SSH.

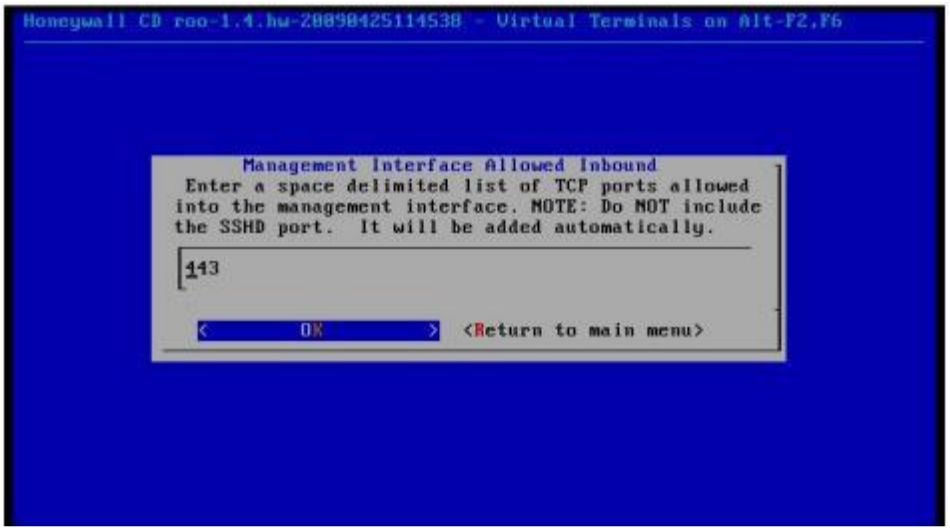


Figura 41: Puerto TCP permitido para acceder a la administración web del Honeywall

Ingresar el rango de direcciones IPs que pueden tener acceso a la administración.

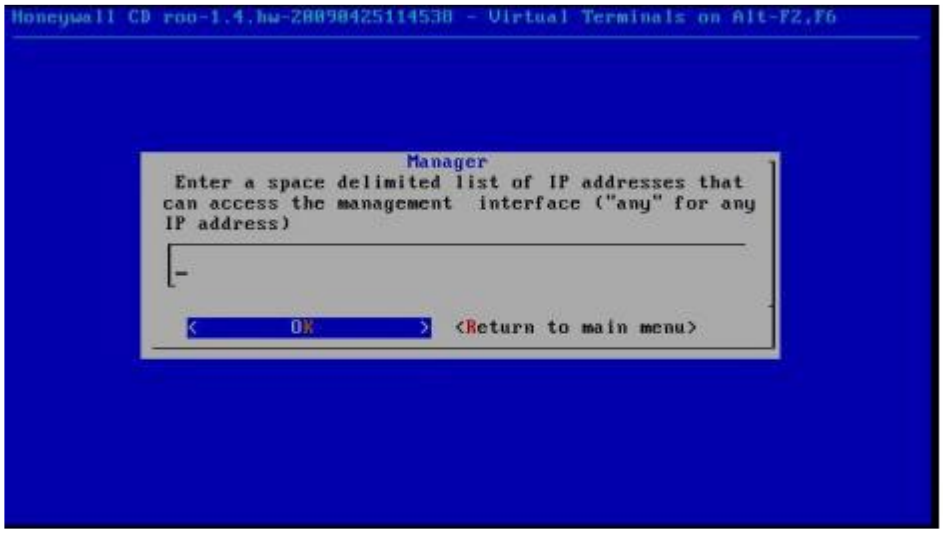


Figura 42: Ingreso de la IP para acceder a la web de administración.

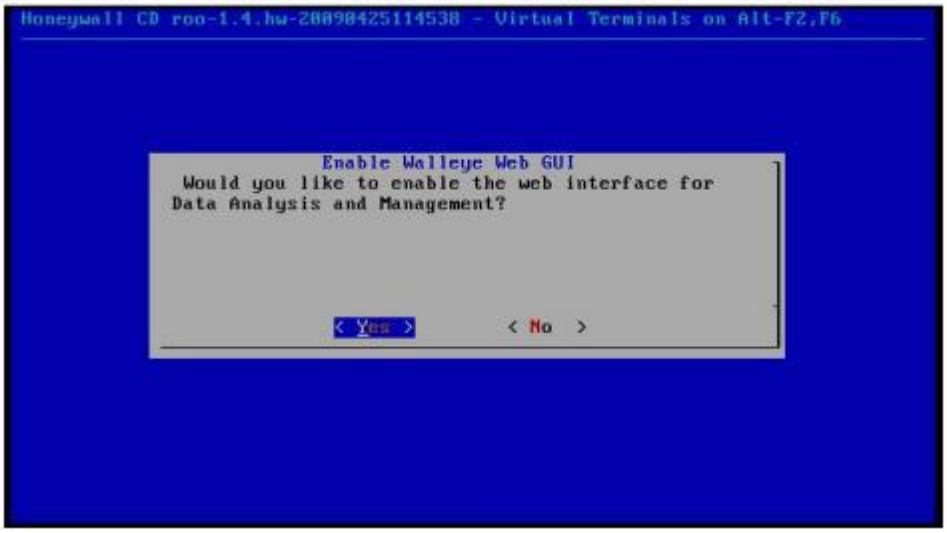


Figura 43: Habilitar la interfaz web de administración.

Activar las restricciones del firewall para prevenir troyanos y malware.

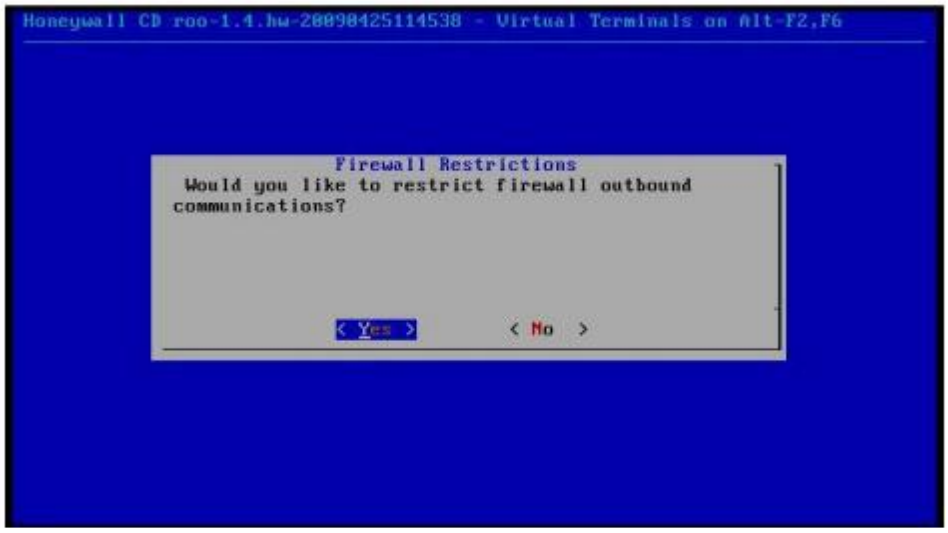


Figura 44: Restricciones de Firewall.

Ingrese la lista de puertos TCP necesarios de salida.

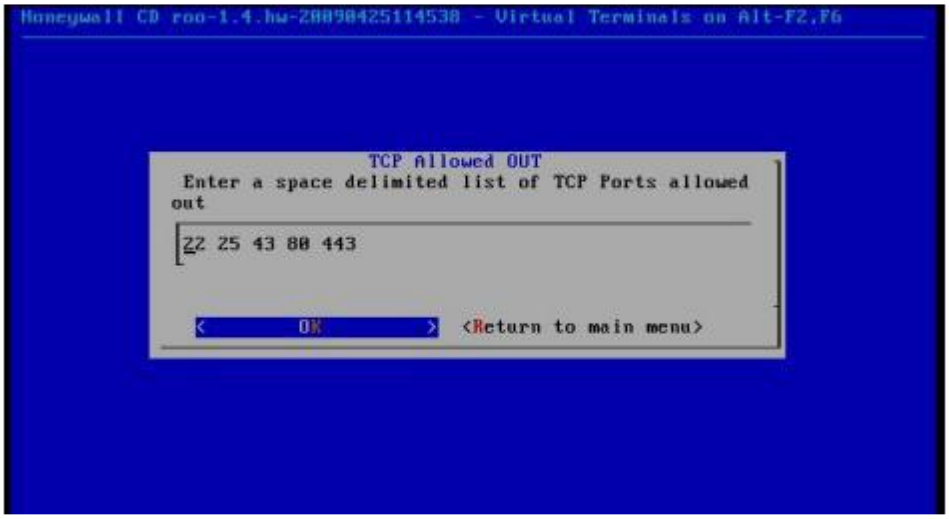


Figura 45: Puertos TCP de salida.

Ingrese la lista de puertos UDP necesarios de salida.

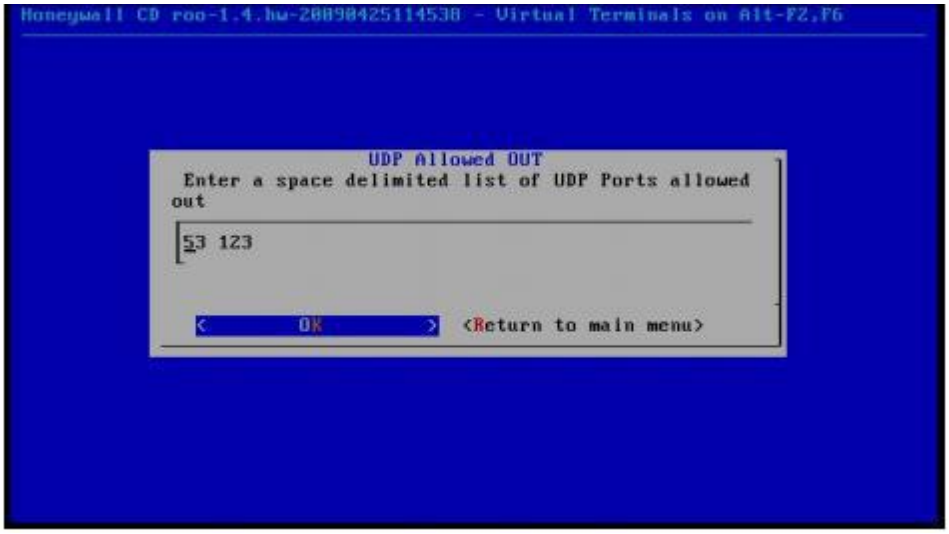


Figura 46: Puertos UDP de salida.

Configuración del límite de Conexiones Permitidas

Se especifica el límite de conexiones por unidad de tiempo (segundo, minuto, hora, día y mes).

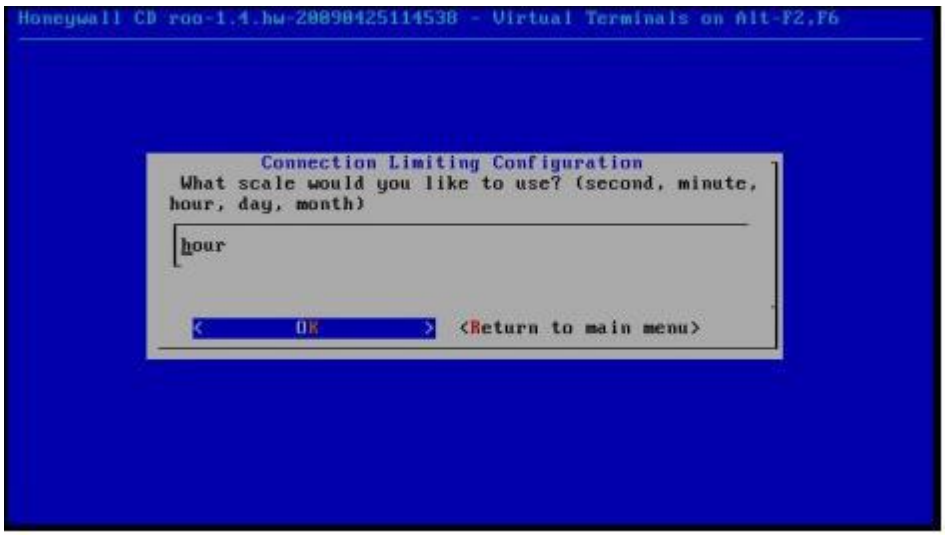


Figura 47: Límite de conexiones (h, m, s).

Especificar el numero de Conexiones TCP que se permiten.

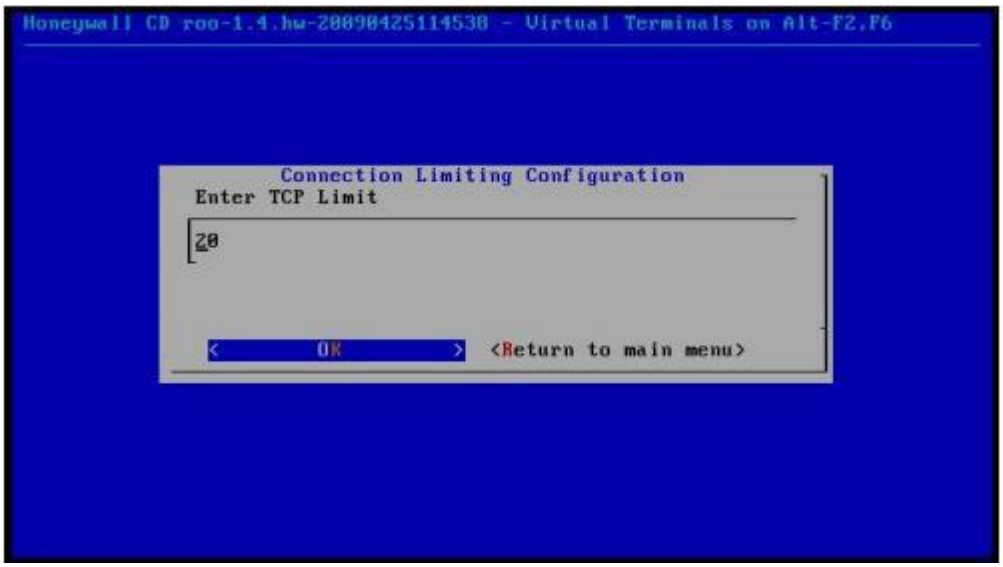


Figura 48: Límite de conexione TCP.

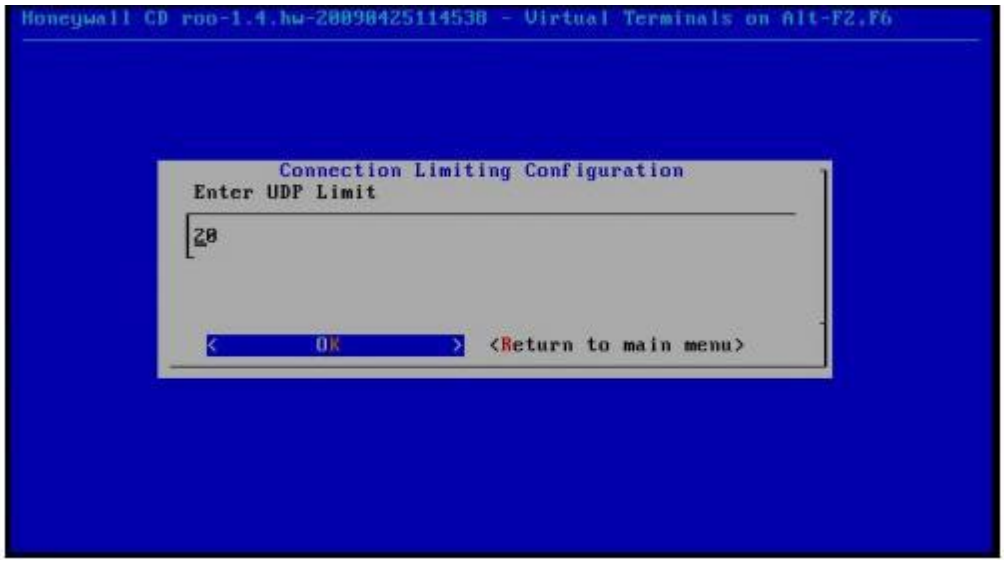


Figura 49: Límite de Conexiones UDP.

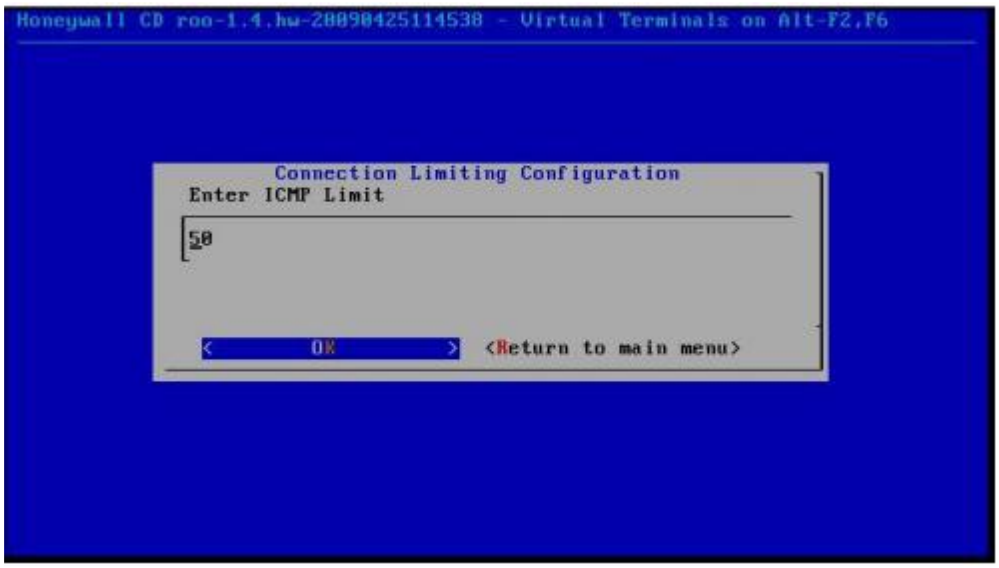


Figura 50: Límite de Conexiones ICMP.

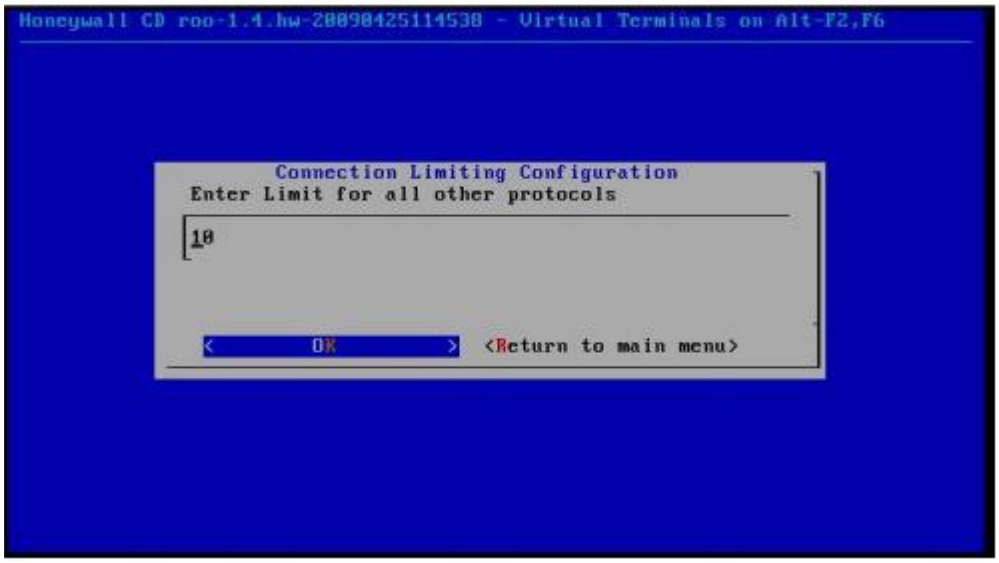


Figura 51: Límite de Conexiones otros Protocolos.

Activar el snort-inline para evitar el tráfico malicioso a la red.

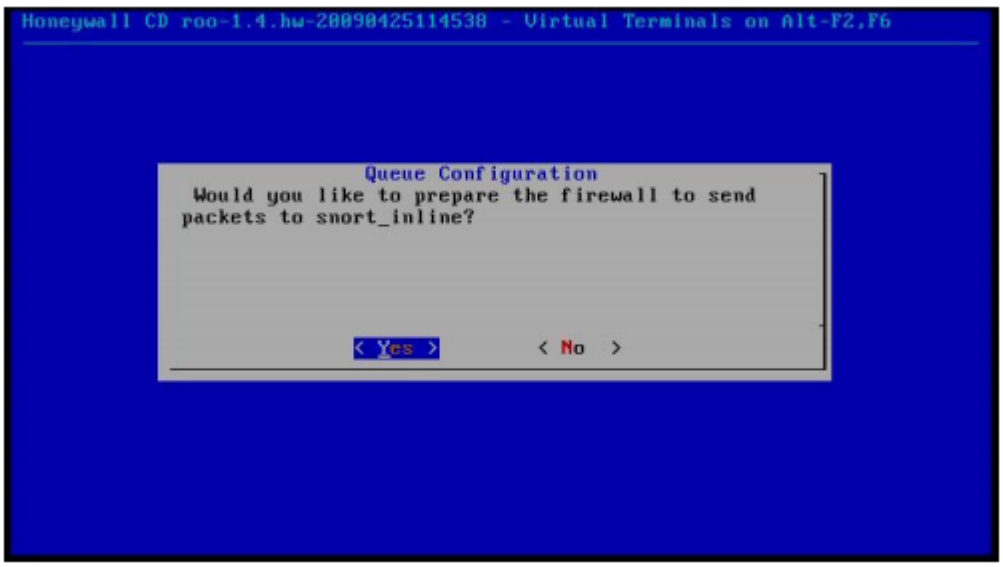


Figura 52: Activación de Snot-inline.

Ingresar el nombre del archivo que contiene la lista de direcciones IPs que generan SPAM (Blacklist).

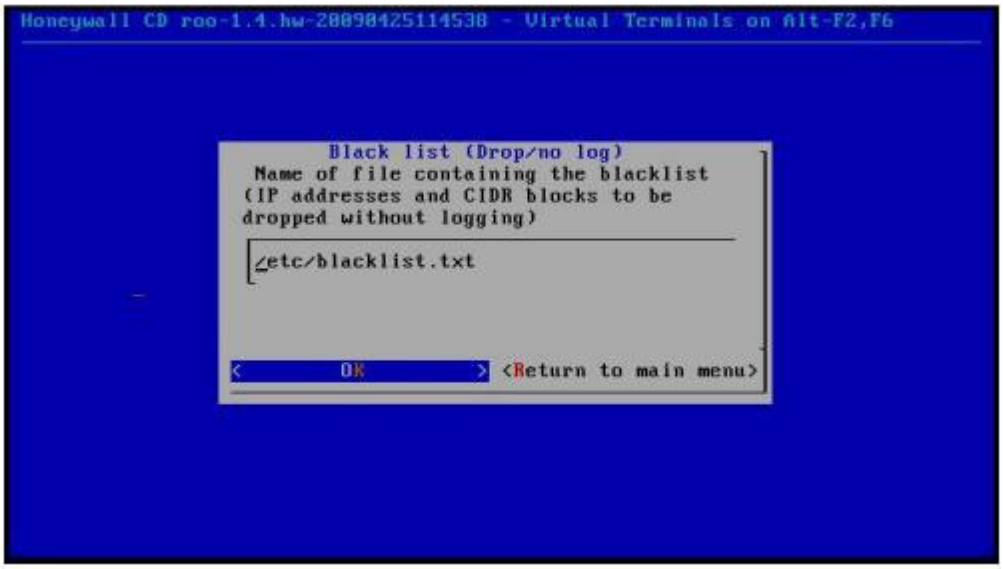


Figura 53: Dirección del Archivo Blacklist

Ingresar el nombre del archivo que contiene las direcciones IPs que nunca generan SPAM (WhiteList).

Figura 54: Dirección del Archivo Whitelist

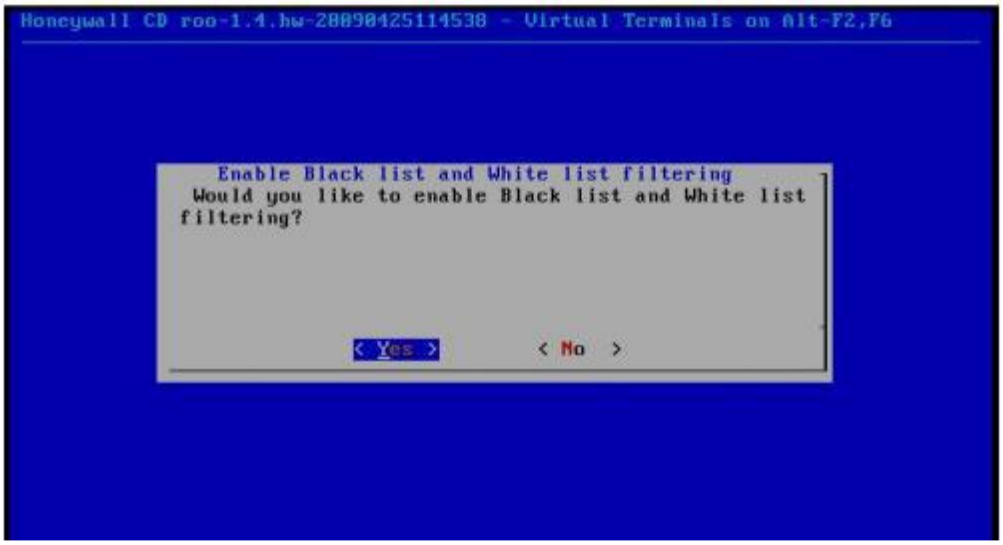


Figura 55: Filtrado de la lista Blanca y Negra.

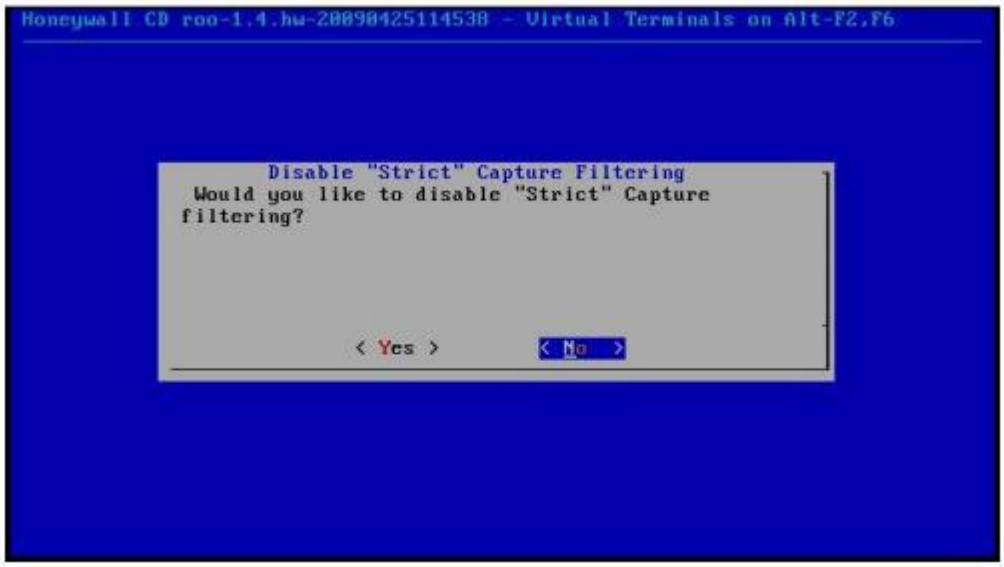


Figura 56: Habilitar “Strict” Capture Filtering

FENCELIST: La finalidad de este fichero es para configurar IPTABLES para registrar y bloquear tráfico de salida hacia otros equipos o redes.

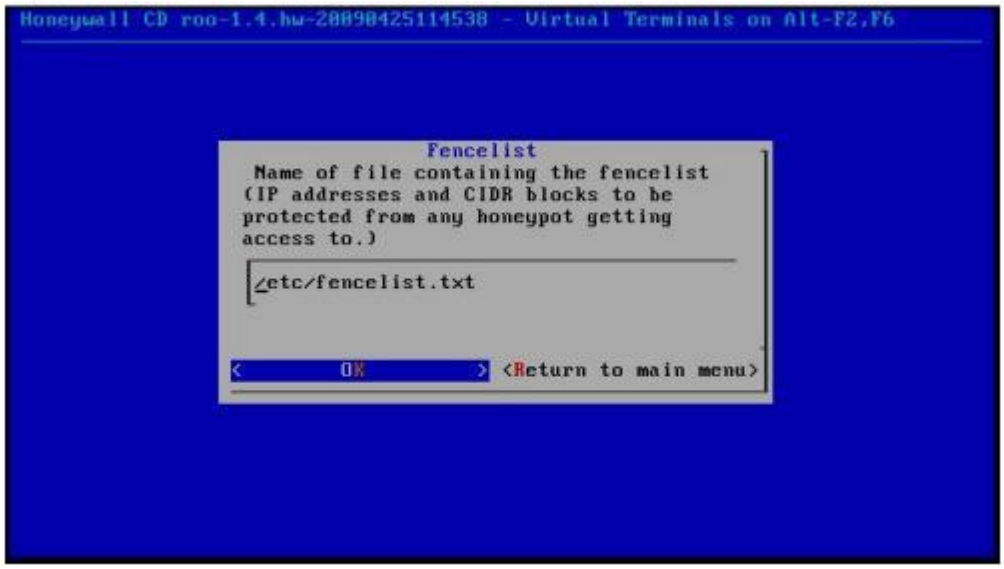


Figura 57: Nombre del Archivo de FENCELIST

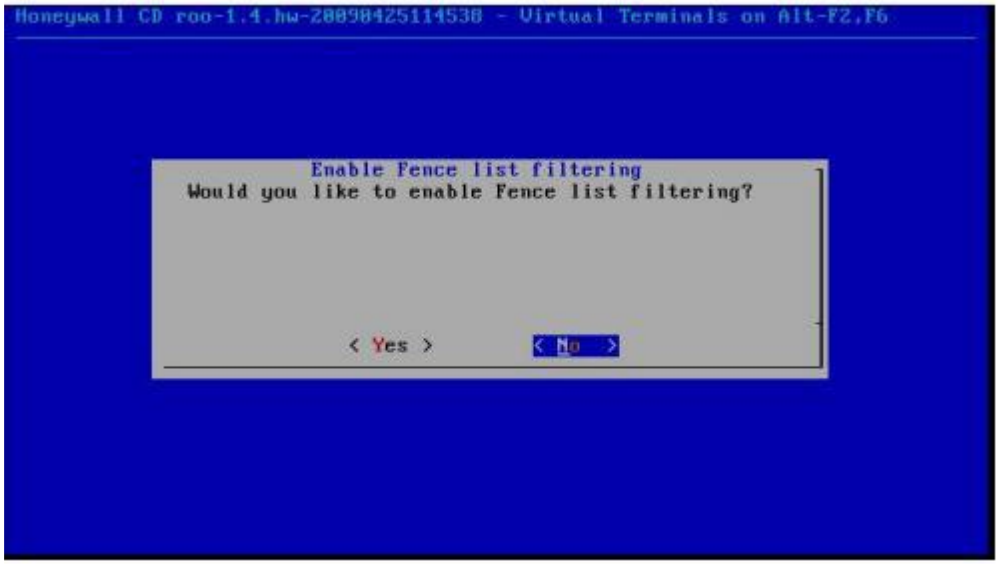


Figura 58: Habilitar FenceList

No habilitar “Roach Motel” para asi desactivar el bloqueo de todo el tráfico saliente de los Honeypots.

Figura 59: Habilitar Roach Motel

Configuración de DNS

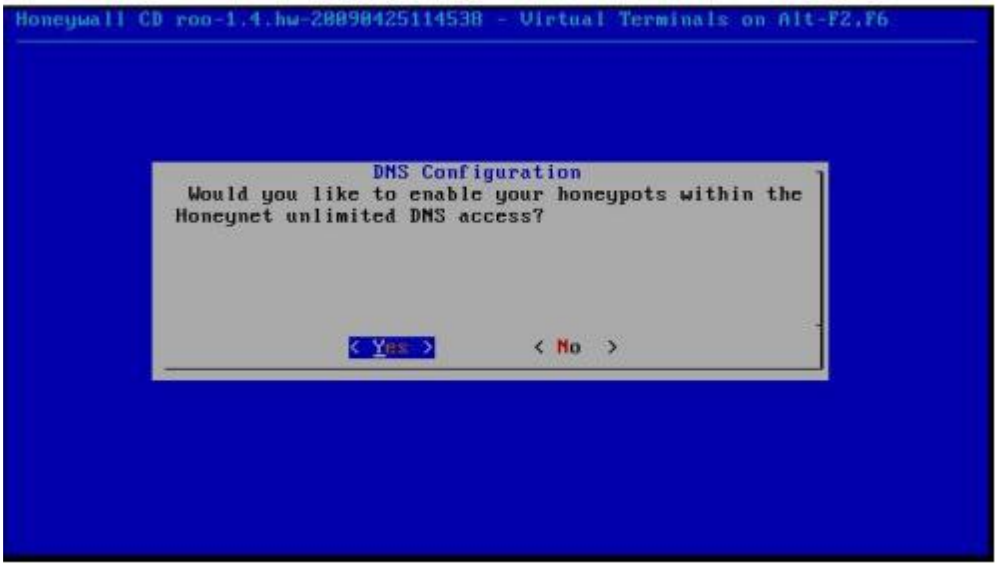


Figura 60: Configuración de los DNS para los Honeypots

Ingresar la lista de las direcciones IPs de los Honeypots.

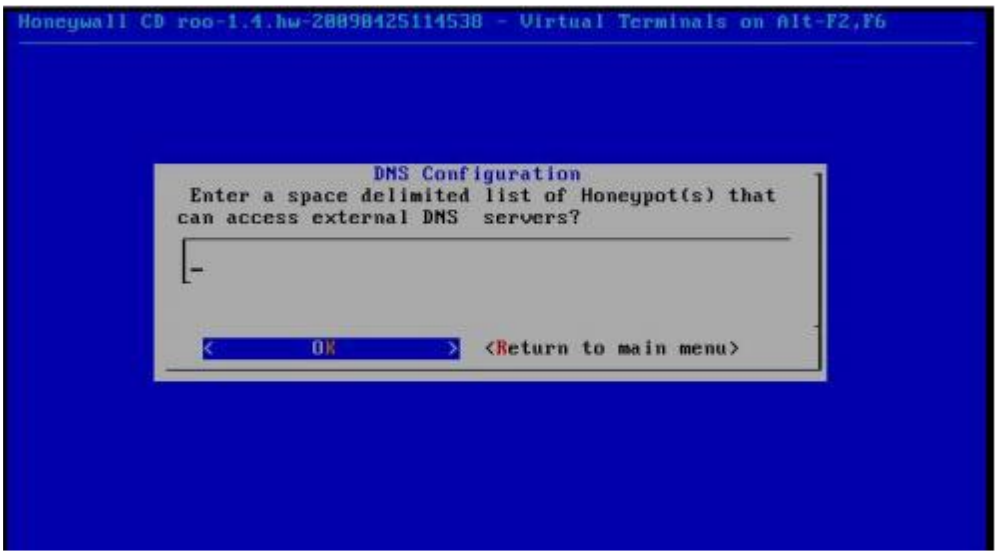


Figura 61: Ip's de los Honeypots

Configuración de DNS server que serán usados para no limitar el acceso.

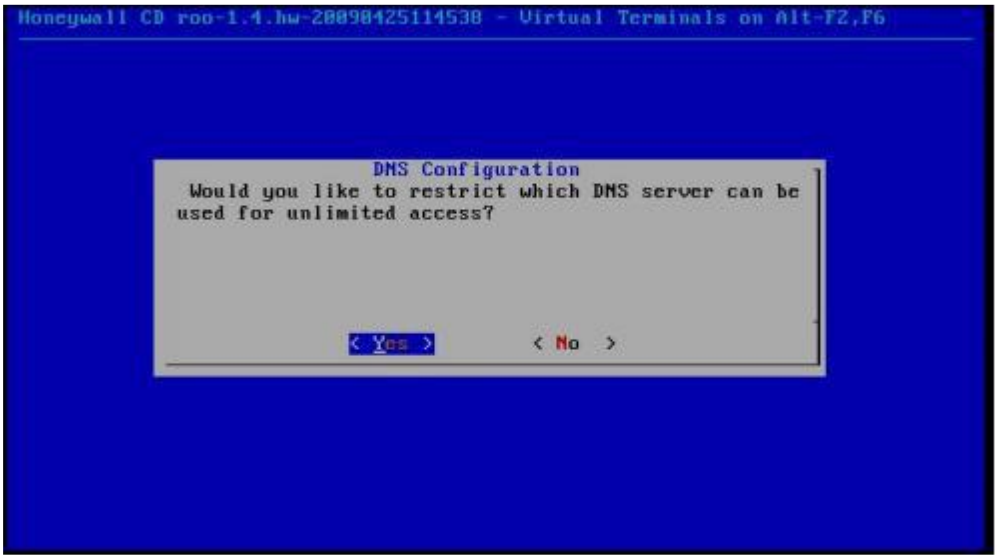


Figura 62: Configuración Servidor DNS

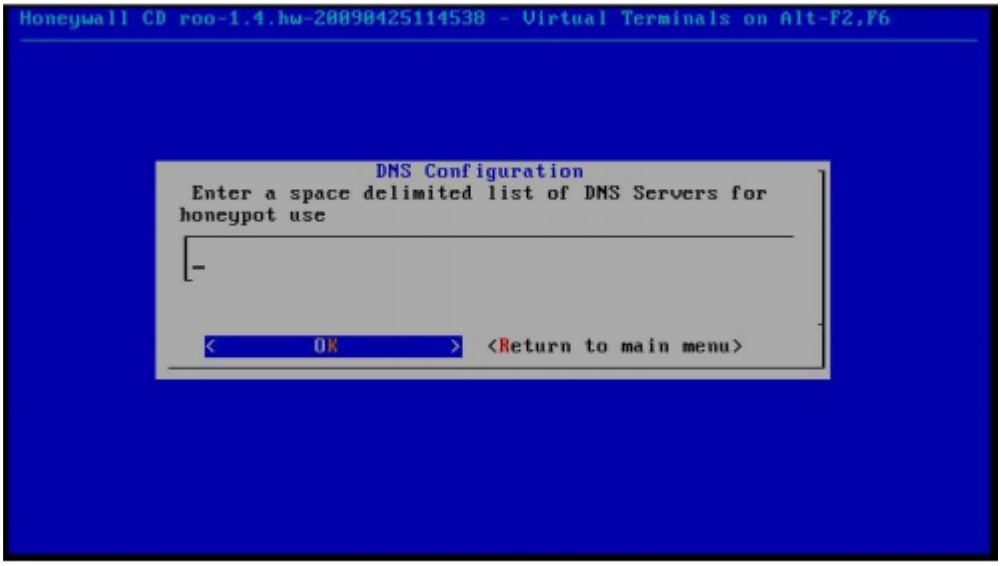


Figura 63: IP del servidor DNS para el Honeypot

Configuración de Alertas.

Figura 64: Configuración de Alertas de mail

Figura 65: Correo electrónico usado para recibir alertas

Figura 66: Finalización de la Configuración del Honeywall

Anexo 5: Configuración e Instalación de los Servicios.

Servidor DHCP

1. Instalar el paquete de dhcp meditante el siguiente comando:
   yum install dhcp.

2. Copiar el archivo de ejemplo que viene en el paquete hacia /etc/dhcpd.conf
   cp /usr/share/doc/dhcp*/dhcpd.conf.sample /etc/dhcpd.conf

3. Editar el archivo dhcpd.conf, el cual debe quedar de la siguiente manera:

```
ddns-update-style interim;
ignore client-updates;
subnet 10.1.28.0 netmask 255.255.252.0 {
        option routers 10.1.28.1;
        option subnet-mask 255.255.252.0;
        option domain-name "deee.espe.edu.int";
        option domain-name-servers 10.1.28.200;
              range 10.1.28.100 10.1.28.254;
              default-lease-time 86400;
              max-lease-time 608400;
}
```

4. Configurar la interfaz por la cual se dara el servicio DHCP, editando el archivo /etc/sysconfig/dhcpd:

```
# Command line options here
DHCPDARGS=eth1
```

5. Iniciar el servicio mediante el siguiente comando:

   service dhcpd start
   chkconfig dhcpd on

Servidor FTP

1. Instalar el paquete tecleando en la terminal el siguiente comando: # yum install -y vsftpd
2. Configurar el archivo que se encuentra en el siguiente directorio /etc/vsftpd/vsftpd.conf.

   Habilitar el usuarios anónimo:

   anonymous_enable=YES|NO

   Habilitar le autenticación local de usuarios

   local_enable=YES|NO

   Habilitar la escritura en el servidor FTP

   write_enable=YES|NO

   Establecer los permisos de escritura, lectura y ejecución.

   local_umask=022

3. Iniciar el servicio, mediante el siguiente comando:
   Service vsftpd start

   Chkconfig vsftpd on

Anexo 6: Certificación de la traducción echa al Resumen del Informe Final.

LIILIANA FERNANDA CELI CELI

English Teacher and Translator. Bachelor's Degree

Certifica:

Que el presente trabajo es una traducción oficial del idioma Español al Ingles de la tesis titulada "Diseño e Implementación de una Honeynet para la red de datos de la Universidad Nacional de Loja, utilizando software libre" del señor Carlos Mauricio Heredia Terán egresado de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja.

Dado y firmado el día 05 de agosto de 2015

Liliana Celi

Número de Registro: 1008-11-1079469

Anexo 7: Licencia Creative Commons.